CFQ IDU

User Interface Manual

© 2009 AS SAF Tehnika.

This book and the information contained herein is the proprietary and confidential information of AS SAF Tehnika. No part of this document may be disclosed, reproduced, or transmitted in any form or by any means, electronic or mechanical, for any purpose without the express written permission of AS SAF Tehnika, 24a, Ganibu Dambis, Riga LV-1005, Latvia.

For permissions, contact SAF Tehnika via e-mail techsupport@saftehnika.com.

Notice of Disclaimer

The information and specifications provided in this document are subject to change without notice. SAF Tehnika reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

Trademark Information

Java™ is a trademark of Sun Microsystems, Inc.

Windows® is a registered trademark of Microsoft Corporation.

All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

Revision History

Date	***Revision***	***Comments***
16.05.2006.	1.0	Initial release
20.06.2007.	1.1	Software components description added, p. 3.3.15
15.09.2008	1.2	Revision and Corrections
12.06.2009	1.3	Revision and Expansion

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

Table of Contents

Table of Contents 3
1 Introduction 9
1.1 Overview 9
1.2 Modes of User Interfaces 9
1.3 Features Overview 9
1.4 Security Measures 10
2 Getting Started 11
2.1 NMS Station Configuration 11
2.1.1 System Requirements 11
2.1.1.1 Local 11
2.1.1.2 Serial 11
2.1.1.3 Network 11
2.1.1.4 Remote 11
2.1.1.4.1 Serial 12
2.1.1.4.2 Network 12
2.1.2 Network 12
2.1.3 Web browser 13
2.1.4 Telnet/SSH client 13
2.1.5 SNMP 14
2.1.6 HyperTerminal 14
2.1.7 Windows Dialer 14
2.2 Access rights for users 14
2.2.1 User Level 1 – Monitor 14
2.2.2 User Level 2 – Operator 15
2.2.3 User Level 3 – Administrator 15
3 User Interface 17
3.1 Overview 17
3.1.1 WEB Overview 17
3.1.2 CLI Overview 18
3.1.2.1 How to use CLI screens 19
3.1.2.1.1 Menu Screens 19
3.1.2.2 Configurable Screens 20
3.1.3 SNMP Overview 22
3.1.3.1 MIBs 22
3.1.3.2 SNMP Agent 22
3.1.3.3 Parameters 22
3.1.3.3.1 SNMP Mode 23
3.1.3.3.2 Trap Version 23

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.1.3.3.3 Auth Trap Enable 23
3.1.3.3.4 Read Community 24
3.1.3.3.5 Write Community 24
3.1.3.3.6 Trap community 24
3.1.3.3.7 SNMP Auth Password 24
3.1.3.3.8 SNMP Priv Password 24
3.1.3.3.9 Trap Manager 24
3.2 Navigation Tree 24
3.3 UI Screens 26
3.3.1 Starting Information 26
3.3.1.1 Description 27
3.3.2 Status Panel 28
3.3.2.1 Description 28
3.3.3 General Network Configuration 29
3.3.3.1 Description 29
3.3.3.2 WEB Configuration 30
3.3.3.3 CLI Configuration 30
3.3.3.4 SNMP Configuration 31
3.3.4 SNMP Configuration 31
3.3.4.1 Description 32
3.3.4.2 WEB Configuration 32
3.3.4.3 CLI Configuration 33
3.3.4.4 SNMP Configuration 33
3.3.5 Syslog Configuration 34
3.3.5.1 Description 34
3.3.5.2 WEB Configuration 34
3.3.5.3 CLI Configuration 35
3.3.5.4 SNMP Configuration 35
3.3.6 E-mail Configuration 36
3.3.6.1 Description 36
3.3.6.2 WEB Configuration 37
3.3.6.3 CLI Configuration 37
3.3.6.4 SNMP Configuration 37
3.3.7 STP Data Configuration 38
3.3.7.1 Description 38
3.3.7.2 WEB Configuration 38
3.3.7.3 CLI Configuration 39
3.3.7.4 SNMP Configuration 39
3.3.8 STP NMS Configuration 39
3.3.8.1 Description 40
3.3.8.2 WEB Configuration 40
3.3.8.3 CLI Configuration 40
3.3.8.4 SNMP Configuration 40
3.3.9 Serial Configuration 41
3.3.9.1 Description 41
3.3.9.2 WEB Configuration 41

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.9.3 CLI Configuration 41
3.3.9.4 SNMP Configuration 42
3.3.10 Device Information 43
3.3.10.1 Description 43
3.3.11 Device Names 44
3.3.11.1 Description 44
3.3.11.2 WEB Configuration 45
3.3.11.3 CLI Configuration 45
3.3.11.4 SNMP Configuration 45
3.3.12 Set Date and Time 46
3.3.12.1 Description 46
3.3.12.2 WEB Configuration 47
3.3.12.3 CLI Configuration 47
3.3.12.4 SNMP Configuration 47
3.3.13 Serial Number Information 48
3.3.13.1 Description 48
3.3.13.2 WEB Configuration 48
3.3.13.3 CLI Configuration 49
3.3.14 Security Configuration 49
3.3.14.1 Description 49
3.3.14.2 WEB Configuration 50
3.3.14.3 CLI Configuration 50
3.3.14.4 SNMP Configuration 50
3.3.15 Reprogramming CPU 51
3.3.15.1 Description 51
3.3.16 WEB Configuration 53
3.3.16.1 CLI Configuration 53
3.3.16.2 SNMP Configuration 53
3.3.17 Add User Entry: 54
3.3.17.1 Description 54
3.3.17.2 WEB Configuration 54
3.3.17.3 CLI Configuration 55
3.3.17.4 SNMP Configuration 55
3.3.18 Delete / Edit User Entry 56
3.3.18.1 Description 56
3.3.18.2 CLI Configuration 57
3.3.18.3 WEB Configuration 57
3.3.18.4 SNMP Configuration 58
3.3.19 View Event Log 58
3.3.19.1 Description 58
3.3.20 Restore System Defaults 59
3.3.20.1 Description 59
3.3.20.2 WEB Configuration 59
3.3.20.3 CLI Configuration 59
3.3.20.4 SNMP Configuration 60
3.3.21 System Reboot 60

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.21.1 Description 60
3.3.21.2 WEB Configuration 60
3.3.21.3 CLI Configuration 61
3.3.21.4 SNMP Configuration 61
3.3.22 E1 / T1 Channel Map 61
3.3.22.1 Description 62
3.3.22.2 WEB Configuration 62
3.3.22.3 CLI Configuration 62
3.3.22.4 SNMP Configuration 63
3.3.23 E1 / T1 Ports 64
3.3.23.1 Description 64
3.3.23.2 WEB Configuration 65
3.3.23.3 CLI Configuration 65
3.3.23.3.1 E1 / T1 Active Channel Screen: 65
3.3.23.3.2 E1 / T1 Configuration Screen 66
3.3.23.4 SNMP Configuration 67
3.3.24 Voice Code 67
3.3.24.1 Description 68
3.3.24.2 WEB Configuration 68
3.3.24.3 CLI Configuration 68
3.3.24.4 SNMP Configuration 69
3.3.25 STM1/OC3 Channel Map 69
3.3.25.1 Description 69
3.3.25.2 WEB Configuration 70
3.3.26 STM1/OC3 Ports 70
3.3.26.1 Description 70
3.3.26.2 WEB Configuration 71
3.3.26.3 CLI Configuration 71
3.3.26.4 SNMP Configuration 71
3.3.27 Authorization 72
3.3.27.1 Description 72
3.3.27.2 WEB Configuration 72
3.3.27.3 CLI Configuration 73
3.3.27.4 SNMP Configuration 73
3.3.28 Configuration Summary 73
3.3.29 Tx Mute Configuration 74
3.3.29.1 Description 74
3.3.29.2 WEB Configuration 75
3.3.29.3 SNMP Configuration 75
3.3.30 APC Configuration 75
3.3.30.1 Description 76
3.3.30.2 WEB Configuration 76
3.3.30.3 SNMP Configuration 76
3.3.31 Protection Configuration 77
3.3.31.1 Description 77
3.3.31.2 WEB Configuration 77

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.31.3 SNMP Configuration 78
3.3.32 Link Configuration Wizard 78
3.3.32.1 Link Wizard Description 78
3.3.32.2 WEB Configuration 79
3.3.32.3 CLI Configuration 80
3.3.32.4 SNMP Configuration 81
3.3.33 ODU Power 82
3.3.33.1 Description 82
3.3.33.2 WEB Configuration 82
3.3.34 ODU Channel selection 83
3.3.34.1 ODU Wizard Description 83
3.3.34.2 WEB Configuration 83
3.3.34.3 CLI Configuration 84
3.3.34.4 SNMP Configuration 85
3.3.35 ODU Configuration 85
3.3.35.1 Description 86
3.3.35.2 WEB Configuration 86
3.3.36 Alarm Threshold 87
3.3.36.1 Description 87
3.3.36.2 WEB Configuration 87
3.3.36.3 SNMP Configuration 88
3.3.37 Alarm Configuration 88
3.3.37.1 Description 89
3.3.37.2 WEB Configuration 89
3.3.37.3 SNMP Configuration 89
3.3.38 Alarm History 90
3.3.38.1 Description 90
3.3.39 Active Alarms 91
3.3.39.1 Description 91
3.3.40 Graphs 92
3.3.40.1 Description 96
3.3.40.2 WEB Configuration 96
3.3.40.3 SNMP Configuration 97
3.3.41 Statistics – Data Switch 97
3.3.41.1 Description 97
3.3.41.2 WEB Configuration 98
3.3.41.3 CLI Configuration 98
3.3.41.4 SNMP Configuration 98
3.3.42 Statistics – NMS Switch 99
3.3.42.1 Description 99
3.3.42.2 WEB Configuration 100
3.3.42.3 CLI Configuration 100
3.3.42.4 SNMP Configuration 100
3.3.43 BERT Mode 101
3.3.43.1 Description 101
3.3.43.2 WEB Configuration 102

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.44 CW Mode 103
3.3.44.1 Description 103
3.3.44.2 WEB Configuration 103
3.3.44.3 SNMP Configuration 103
3.3.45 Loopback 104
3.3.45.1 Description 104
3.3.45.2 WEB Configuration 104
3.3.45.3 CLI Configuration 104
3.3.45.4 SNMP Configuration 105
3.3.46 Modem Temperature 105
3.3.46.1 SNMP Configuration 105
3.3.47 Logout: 105
3.3.47.1 Description 106
3.4 Uploading Files to IDU 106
3.4.1 File Upload using *iPorter* Program 106
3.4.2 File Upload using Internet Browser 106
4 Troubleshooting 107
4.1 Cannot access IDU using IP (Web / Telnet / SSH) 107
4.2 The web page resolution is improper 107
4.3 Unable to establish a secure connection 107
4.4 Unable to access different network services 107
5 Appendix 109
5.1 Abbreviations & Acronyms 109
5.2 References and Links 111
5.2.1 Install Mozilla Firefox 111
5.2.2 Install Internet Explorer 111
5.2.3 Install Java 112
5.2.4 Install PuTTY 112

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

1 Introduction

1.1 Overview

The User Interface Manual explains the different user interfaces for accessing and configuring the CFQ IDU.

1.2 Modes of User Interfaces

The terminal can be accessed through Serial, Ethernet, or Modem interfaces using the following modes:

- Web Interface (Normal / SSL)
- Command Line Interface, CLI (Telnet/ SSH)
- SNMP Agent

1.3 Features Overview

- CFQ IDU Provisioning
  - Network Time Protocol (NTP) client
  - Spanning-Tree Protocol (STP) configuration
  - SNMP configuration
  - Serial port configuration
  - Security configuration
  - Configuration saving/retrieving
  - Feature authorization
  - Configuration saving/retrieving
  - Alarm notification configuration
  - E-mail
  - DHCP client for automated NMS network configuration
- Link Provisioning
  - Modulation, Bandwidth, E1 channels, Ethernet, STM-1
- Status and Monitoring
  - Automated alarm reporting

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

  - Eb/N0, RSL, Errored-Seconds
  - Event Log
  - Alarm Log
  - Remote logging to Syslog server
  - SNMP TRAPs
- Firmware Upgrade
- User Management

1.4 Security Measures

The software allows for partitioning resources and prohibiting access of sensitive information. The design of the software also prevents users from intruding on other users and/or resources on the network. Security measures include

- Encrypted passwords
- Multilevel configuration permissions
- Network data encryption
- Accounting and logging features provide protection from and information about access attempts.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

2 Getting Started

2.1 NMS Station Configuration

2.1.1 System Requirements

2.1.1.1 Local

Local connection of a PC to a CFQ IDU can be accomplished via a serial or network port. The connection requirements are listed below.

2.1.1.2 Serial

- PC with serial port and DB-9 to HD-15 CFQ IDU cable
- Serial communications software (e.g. Hyperterm)

2.1.1.3 Network

- PC with 10/100 Ethernet interface
- CAT 5 patch cable for connecting PC to CFQ IDU NMS port
- Internet Explorer 5.5 or higher, or
- Telnet or SSH client, or
- SNMP manager

2.1.1.4 Remote

Remote connection from a PC to a CFQ IDU can be accomplished via a serial communication connection or an internet connection. The connection requirements are listed below.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

2.1.1.4.1 Serial

- PC with modem
- Serial communications software with dialer (e.g. Hyperterm)
- External modem connected to CFQ IDU with DB-9 to HD-15 CFQ IDU cable

2.1.1.4.2 Network

- PC with internet connection
- Remote CFQ IDU with publicly addressable IP address
- Internet Explorer 5.5 or higher, or latest mozilla firefox browser, or
- Telnet or SSH client, or
- SNMP manager

2.1.2 Network

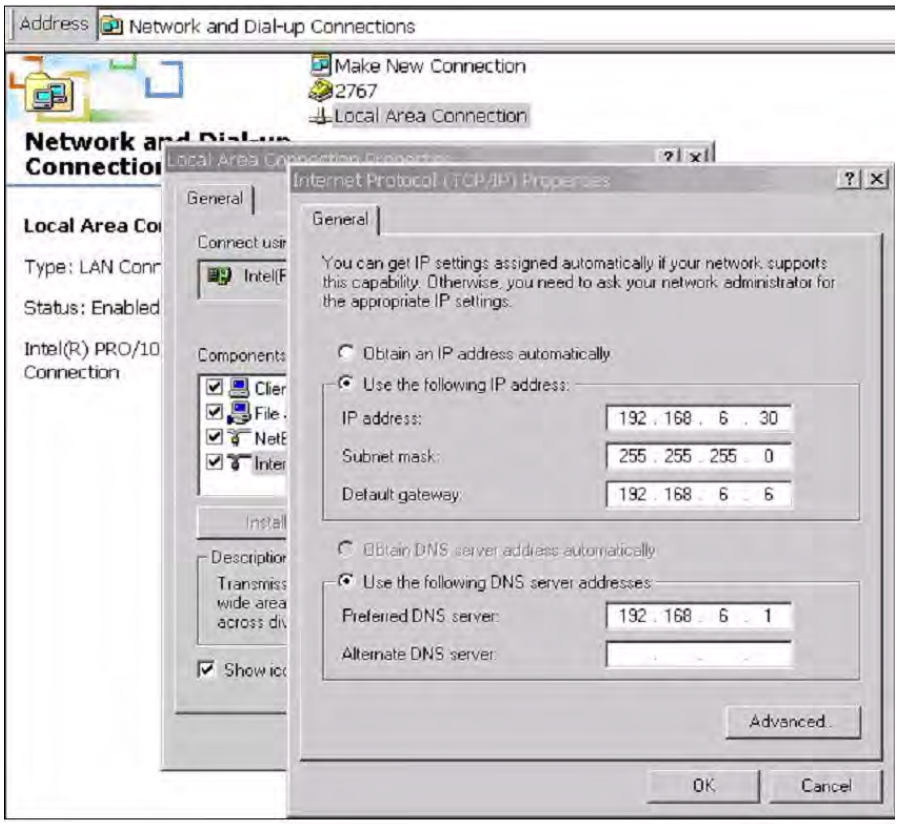

Address
Network and Dial-up Connections
Make New Connection
2767
Local Area Connection
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 6 . 30
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 6 . 6
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 6 . 1
Alternate DNS server:
Advanced...
OK
Cancel

Figure 2.1. Network connections.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

To set up a network connection

- Access the TCP/IP properties from the control panel network connection menu as shown in Figure 2.1. Verify the IP address, net mask, gateway, and DNS
- Server settings.
- Execute a ping to verify connectivity, by typing “ping” followed by the target unit IP address at a command prompt.

2.1.3 Web browser

When accessing the software via the web interface, use one of the following web browsers

- Use Internet Explorer version 5.5 or above
- Mozilla Firefox (latest version preferred)

Use the browser’s default settings.

Refer to Section 5.2.1 and Section 5.2.2 for instructions for obtaining a web browser.

The web interface also requires the use of Sun Java JVM version 1.2.2 or above. Refer to Section 5.2.3 for instructions for obtaining Sun Java JVM.

2.1.4 Telnet/SSH client

When accessing the software via the CLI interface, use a telnet or SSH client. An SSH client is similar to a telnet client except it accesses the target over a secure connection.

Windows provides a Windows Standard telnet client that may be accessed through the command prompt. An alternate telnet client may be used.

Refer to Section 5.2.4 for downloading PuTTY, a popular Telnet / SSH Client for Windows.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

2.1.5 SNMP

Configure SNMP manager for accessing the Target (Connected Product).

2.1.6 HyperTerminal

When connecting via a HyperTerminal program, use the following settings:

- BaudRate=38400
- Parity=none
- DataBit=8
- StopBit=1

The settings may be reconfigured based on system requirements.

2.1.7 Windows Dialer

The Windows Dialer may be used to connect a CFQ IDU via a telephone and modem. Create a standard dial-up account in Windows and enter the phone number of the telephone connected to the Product.

There is no need to enter username and password while dialing, “dialing” access is not authenticated.

2.2 Access rights for users

The system has five user access levels for configuring and viewing data through user interface. User accounts can be added and deleted for different access levels. The five user levels and their corresponding user rights are described below.

2.2.1 User Level 1 – Monitor

User has minimum access rights and can only view the following pages.

- Home

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

- General Device Information,
- Configuration Summary
- Active Alarm Status
- Alarm History
- All Graphs.

The default username and password for User Level 1 is:

Username: monitor

Password: monitor

2.2.2 User Level 2 – Operator

User has all the access rights of User Level 1 and has additional rights to edit following pages

- Reboot,
- All Radio Link and Data Link Configuration pages
- Alarm Configuration page
- BERT page.

The default username and password for User Level 2 is:

Username: operator

Password: col1ma

2.2.3 User Level 3 – Administrator

User has all the rights of User Level 2 and has additional rights to the following pages

- All Network Configuration
- Serial and Security configuration
- All Device Information pages
- All Maintenance and Restore Defaults pages.
- STP Screens

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

The default username and password for User Level 3 is:

Username: administrator

Password: d1scovery

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3 User Interface

3.1 Overview

3.1.1 WEB Overview

The web interface is a rich feature-filled graphical interface for configuring and monitoring the terminal. Access to web interface is provided via a web browser and a normal or secure connection.

To access the web interface

1. Open a web browser (browser requirements are discussed in Section 2.1.3)
2. Type the IP address of the CFQ IDU in the address bar and press GO.
3. A popup window will prompt for a user name and password.
4. Enter user name and password then press OK.
5. Upon successful authentication, the Starting Information Screen (Figure 3.1) is displayed.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

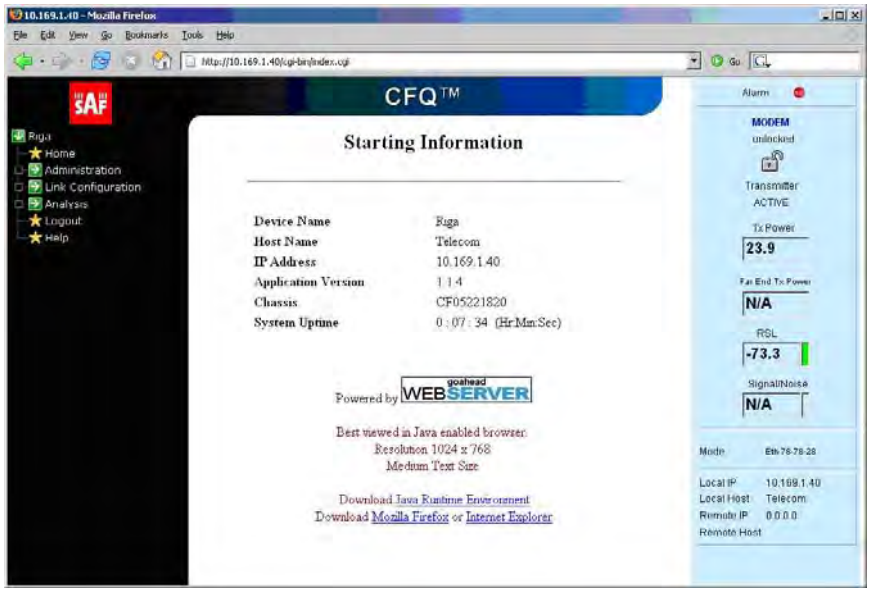


Figure 3.1. Web starting information screen.

3.1.2 CLI Overview

The CLI provides a text based interface for configuring and monitoring the terminal. The CLI is accessed by doing one of the following

Using Ethernet interface,

1. Telnet / SSH to the terminal (using IP address of the terminal),
2. Enter a user name and password at the login prompt.

Using Serial interface,

1. Establish an RS232 connection using a serial terminal
2. Enter a user name and password at the login prompt.

Using Modem interface,

1. A remote user can access the CLI, by using the Windows Dialer to establish a connection and get the terminal IP address
2. Telnet / SSH to the terminal
3. Enter a user name and password at the login prompt.

Upon successful authentication the ”General Information Screen” is displayed (Figure 3.2. CLI starting information screen.). Switch to the “Main Menu” screen

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

by pressing the M-key. From the “Main Menu,” the user can navigate through various interface screens.

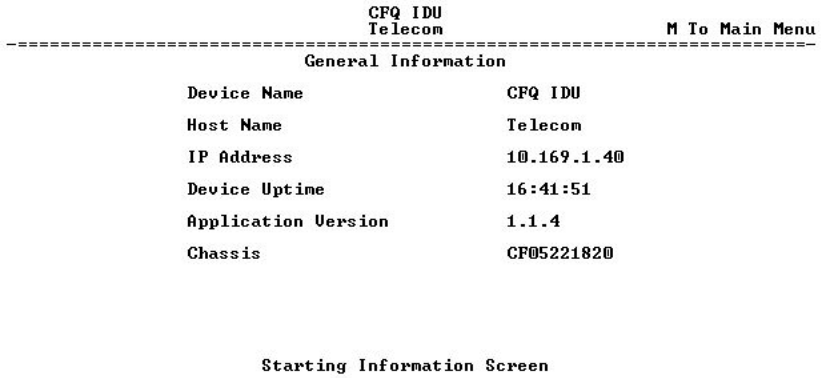


Figure 3.2. CLI starting information screen.

3.1.2.1 How to use CLI screens

3.1.2.1.1 Menu Screens

Menu screens are used to navigate between functions. They display a list of navigation choices. Each choice is listed with a character encased within [ ] braces, or “hotkey.” Press the “hotkey” to switch to the corresponding screen. For example, in Figure 3.3. CLI menu type screens., enter ‘a’ / ‘A’, to switch to the “General Information” screen (the “General Information” screen is displayed in Figure 3.2).

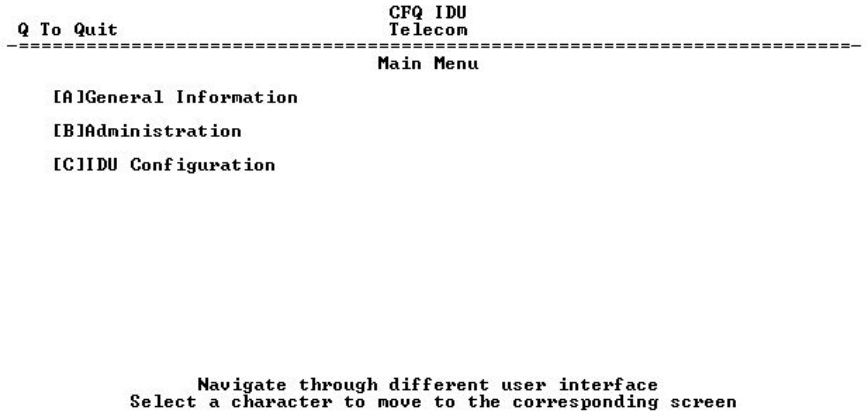


Figure 3.3. CLI menu type screens.

Further references to “hotkey” in this document will refer to the character encapsulated in [ ] brackets for the individual parameter.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.1.2.2 Configurable Screens

Configurable screens are used to set various parameters. Figure 3.4. Configurable Screen. shows the “General Network Configuration” screen, which is an example of a configurable screen. Parameters are listed with their values and a “hotkey.”

Press the “hotkey” to configure the corresponding parameter. For example, enter ‘a’ / ‘A’, to edit IP address, then press “Enter Key”.

Some parameters may have a set list of values. For example, the DHCP Client parameter has two values: Enabled and Disable. To edit this type of parameter, press the corresponding “hotkey” (in this case “E”), then press the “Space Bar”-key, to scroll through different values. Once the desired value is displayed, press the “Enter”-key.

If the parameter is displayed without hotkey, it implies a Read-only parameter.

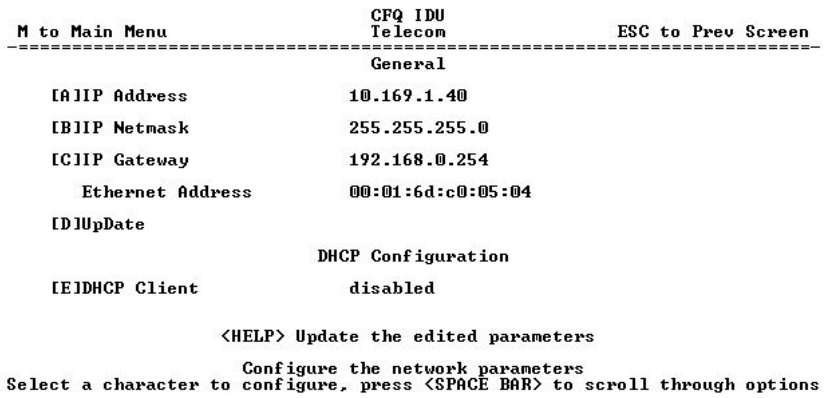


Figure 3.4. Configurable Screen.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

All the CLI screens will have the following messages:

Navigation Message: Help message about possible navigation from the screen. This will be displayed at top left and top right of the screen.

Screen Message: Help message about the screen. This will be displayed at 24th row.

Access Message: Help message about how to access parameters of the screen. This will be displayed at 25th (last) row

In the CLI, there are two different types of parameter updates. Some parameters are updated individually and other are updated as a group.

To perform an **Individual Update**:

1. Edit the parameter value.
2. Press the “Enter”-key.
3. If update was successful, the message “Updated Successfully” will be displayed.
4. If the update failed, a failure message will be displayed.

To perform a **Group Update**:

1. Edit the parameter value.
2. Press the “Enter”-key.
3. Press the character specified for “Update.”
4. If the update was successful, the message “Updated Successfully” will be displayed.
5. If the update failed, a failure message will be displayed.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

1. CLI screens should ideally be viewed at 25x80.
2. A window of less than 25x80 will have incomplete content.

3.1.3 SNMP Overview

The SNMP agent interface provides a means of configuring the terminal using Simple Network Management Protocol (SNMP) commands.

3.1.3.1 MIBs

A Managed Information Base (MIB) file describes a type of device in a network as a data structure. The CFQ-IDU SNMP agent supports the following MIBs.

- **reg.mib:** This MIB file contains the registration for products.
- **SDIDU.mib:** This is the main MIB file for the CFQ IDU product.
- **SDIDU_v1Traps.mib:** CFQ IDU product version 1 trap MIB file
- **SDIDU_v2Traps.mib:** CFQ IDU product version 2 trap MIB file

The SNMP agent interface uses these MIB files to configure the system.

3.1.3.2 SNMP Agent

3.1.3.3 Parameters

The SNMP agent interface configurable parameters are described in the following sections.

WEB and CLI interfaces can be used to configure the SNMP parameters below. Change in any of the parameters below reconfigures the agent.

If the agent is configured in “v3 only” or “v1-v2-v3” mode, SNMPv3 “admin” user can configure the SNMP users. There are 4 possible levels of users. User levels are same as described in Section 2.2.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

The SNMP agent does not support level based access, if the agent is configured as “v1 only” or “v2 only” mode. In the case of v1 and v2 modes of operation, Level1 access is given to the read operation and Level4 access is given for the write operation. Thus in v1 and v2 modes of operation user has full access to system configurations if a valid write community string is used.

3.1.3.3.1 SNMP Mode

The SNMP agent can be configured to operate in any of the following modes

- disable
- v1 only
- v2 only
- v3 only
- v1-v2-v3

If the agent is configured to run as v1 only, v2 only or v3 only, then user can access the agent only using SNMP v1, v2 or v3 respectively.

If the agent is configured to operate in the v1-v2-v3 mode, then user can access the agent using SNMP v1, v2 or v3.

The SNMP agent is disabled by selecting the disable mode.

SNMP v1 and v2 provides a weak security by using the community strings. The user can always configure the SNMP agent to operate in “v3 only” mode, which uses authentication as well as encryption for secure transaction.

3.1.3.3.2 Trap Version

A trap is an SNMP message issued by an SNMP agent that reports an event.

The Trap Version parameter configures the SNMP trap version. The SNMP agent uses the specified version to send the traps to configured trap managers.

3.1.3.3.3 Auth Trap Enable

If enabled, SNMP agent generates Authentication failure trap on authentication failure in any request.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.1.3.3.4 Read Community

A community string is an SNMP security password. The Read Community string is used in read operation of SNMP v1 or v2, and allows the SNMP manager to issue Get and GetNext messages.

3.1.3.3.5 Write Community

The Write Community string is used in write operation of SNMP v1 or v2, and allows the SNMP Manager to issue Set messages.

3.1.3.3.6 Trap community

The Trap Community string allows the SNMP agent to issue Trap messages.

3.1.3.3.7 SNMP Auth Password

The SNMP Auth Password is used in only SNMP v3 mode of operation and is the authorization password for the “admin” user.

3.1.3.3.8 SNMP Priv Password

The SNMP Priv Password is used in only SNMP v3 mode of operation and is the privacy password for the “admin” user.

3.1.3.3.9 Trap Manager

Trap Manager configures the trap managers IP addresses. A maximum of four Trap managers can be configured. The SNMP agent sends the traps to all the configured trap managers

3.2 Navigation Tree

The Navigation tree shown describes location of each user interface screen. Nested screens are indented under the screen from which they can be accessed.

- Home
  - Starting Information
  - Status Panel
- Navigation Tree
  - Administration
    - Network Configuration

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

- General Network configuration
- SNMP Configuration
- Syslog Configuration
- E-mail Configuration
- STP Data Configuration
- STP NMS Configuration

- Serial Configuration
- Security Configuration
- Device Configuration
  - Device Information
  - Device Names
  - Set Date and Time
  - Serial Number Information
- Maintenance
  - Reprogramming CPU
  - Add User
  - Delete User/ Edit User Entry
  - View Event Log
- Restore Default
- Reboot

- Link Configuration
  - Authorization
  - Configuration Summary
  - Data Link
    - E1 / T1 Channel Map
    - E1 / T1 Ports
    - Voice Codec
    - STM-1/OC3 Channel Map
    - STM-1/OC3 Ports
  - Radio Link
    - APC Configuration
    - Protection Configuration
    - ODU TX Mute Configuration
    - Link Configuration
    - ODU Power
    - ODU Channel
    - ODU Configuration
- Analysis
  - Alarms
    - Alarm Threshold
    - Alarm Configuration
    - Alarm History
    - Active Alarms
  - Graphs
  - Statistics
    - Data Switch
    - NMS Switch
  - BERT Mode

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

- CW Mode
- Loopback

c Logout

3.3 UI Screens

Each UI Screen is described in the following sections. Each screen section contains the following components:

- User Access Level - Each screen is labeled with “User Access Level: Level X,” where X refers access rights for a particular user.
- Description – Gives a description of the screen and the parameters it displays/edits.
- Web Configuration – Gives details to access parameters through web browser.
- CLI Configuration – Gives details to access parameters through CLI Telnet / SSH session / Hyper terminal.
- SNMP Configuration – Gives details to access parameters through SNMP manager

Read-only pages are the only exception, as they have no specific details for different interfaces.

3.3.1 Starting Information

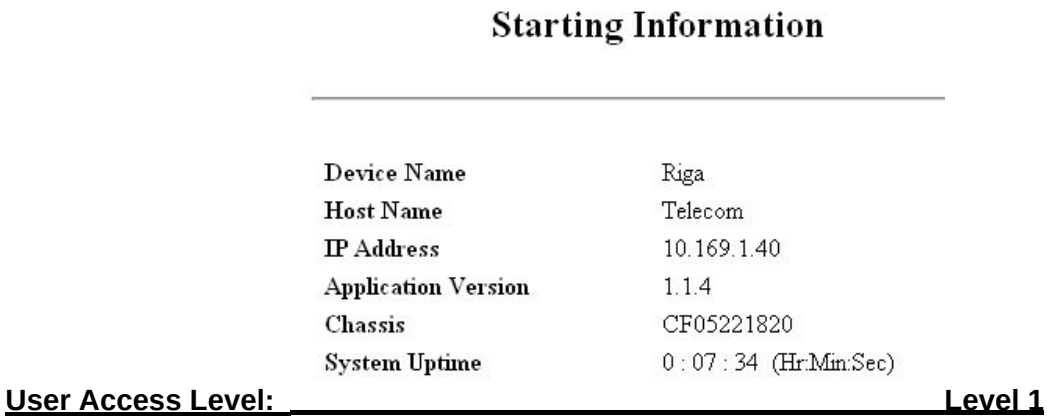


Figure 3.5. Starting Information.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

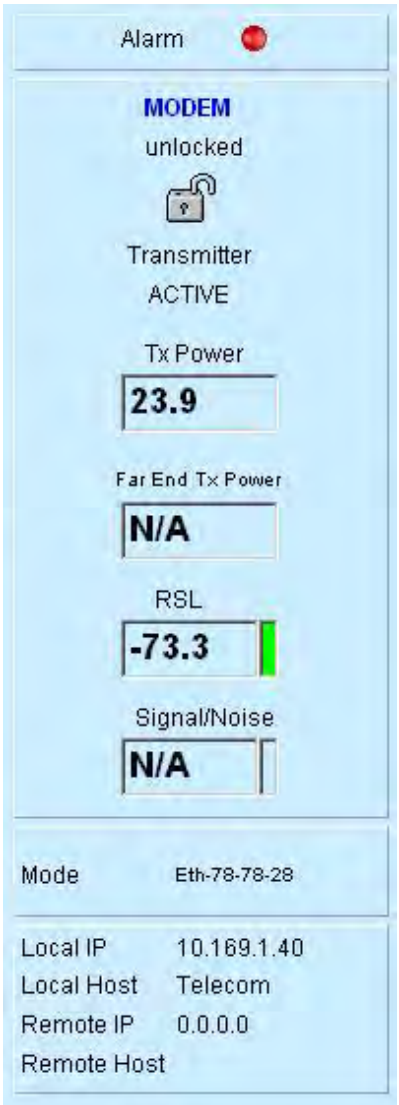
3.3.1.1 Description

Figure 3.5 shows the starting information screen of user interface. This screen provides general information about the CFQ IDU, including

- **Device Name** – Name of the product
- **Host Name** – Name of the host
- **IP Address** - IP Address of the system.
- **Application Version** – Version information of the application
- **Chassis Serial Number** – Serial number of the product (factory assigned).
- **System Uptime** – Uptime of the System.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.2 Status Panel



User Access Level: Level 1

Figure 3.6. Status Panel.

3.3.2.1 Description

Figure 3.6 shows the status panel for 1 + 0 and 1 + 1 configurations. This screen provides the modem and alarm status of the terminal as follows:

1. **ALARM –** Alarm Status
   - **Red LED** indicates an alarm has occurred
   - **Green LED** indicates no alarms in the terminal

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

- Click on the LED to view the “Active Alarms” Page.

2. **East / West MODEM** – MODEM Status
   - **NA** indicates MODEM is inactive
   - **LOCK Symbol** indicates MODEM is locked
   - **UNLOCK Symbol** indicates MODEM is unlocked
3. **TX Power** – Transmitting power of the MODEM in dB.
4. **Far End TX Power** – Far end transmitting power of the MODEM in dB.
5. **CFQ IDU RSL –** RSL value in dBm.
6. **SIGNAL/NOISE –** Signal/Noise value in dB. If Modem is unlocked, this value will not be displayed.
7. **East mode –** Operation mode of the East Link
8. **West mode –** Operation mode of the West Link
9. **Local IDU Information –** IP Address and Host Name
10. **Remote IDU Information –** IP Address and Host Name

3.3.3 General Network Configuration

User Access Level: **Level 3**

Figure 3.7. General Network Configuration.

3.3.3.1 Description

The General Network Configuration screen (Figure 3.7) is used to configure the following general network related parameters:

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

1. **IP Address** - Enter the IP Address for the terminal. If unsure contact your network administrator.
2. **IP Netmask** – Enter the appropriate netmask depending on the class of the network. If unsure contact your network administrator.
3. **IP Gateway** – Enter the gateway IP Address for your subnet. If unsure contact your network administrator.
4. **Ethernet Address –** MAC **or** Hardware address of the terminal.
5. **DHCP Client –** When enabled, network parameters are obtained dynamically from a DHCP server. The other parameters on the page cannot be modified when DHCP is enabled.

3.3.3.2 WEB Configuration

1. Navigate to Administration→Network Configuration and click on the General Menu in the left panel.
2. All General Network related parameters are displayed with current/present values.
3. To revert to previous values, press Reset button.
4. To change parameters, enter new values and press the “update” button.
5. The page is refreshed and displayed with the updated or current/present values.
6. If parameters are not updated with the entered values, the values entered may be invalid for that parameter.

3.3.3.3 CLI Configuration

1. Navigate to Administration→General Network Menu→ Network Configuration
2. All General Network related parameters are displayed with current/present values.
3. To edit an individual parameter, enter its hotkey, edit its value and press the Enter key.
4. To revert to the previous value, press the “Esc” key while editing the value.
5. When editing the DHCP Client parameter, scroll through the options using the Space Bar key and press Enter to select an option.
6. To update the edited parameter, press the hotkey for “Update”.
7. The page is refreshed and displayed with the updated or current/present values.

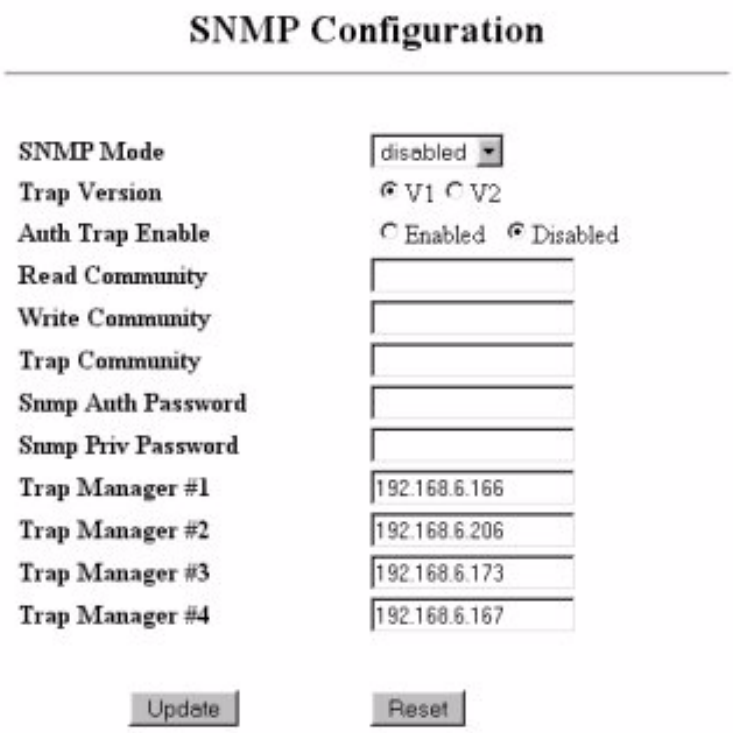
© Copyright 2009 SAF Tehnika A/S All Rights Reserved

8. If parameters are not updated with entered values, the value entered may be invalid for that parameter.

3.3.3.4 SNMP Configuration

1. Select a parameter from the MIB section *SysCfgNetworkIP*
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter.

3.3.4 SNMP Configuration



User Access Level: **Level 3**

Figure 3.8. SNMP Configuration.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.4.1 Description

Figure 3.8 shows the screen used to configure the following SNMP related parameters:

1. **SNMP Mode** – The mode in which SNMP Agent is currently configured.
2. **Trap Version** – The Trap Version in which SNMP Agent is currently configured
3. **Auth Trap Enable** – Enable/Disable sending of authorization traps to SNMP manager.
4. **Read Community** - Community String used while reading data from the SNMP Agent in SNMP V1/V2 mode.
5. **Write Community** - Community String used while writing data to the SNMP Agent in SNMP V1/V2 mode.
6. **Trap Community** - Community String used while sending traps from the SNMP Agent.
7. **SNMP Auth Password** - Password required for authorization while reading or writing data in SNMP V3 Mode.
8. **SNMP Priv Password** - Privacy password required while reading or writing data in SNMP V3 Mode.
9. **Trap Manager #1 - #4** - IP Addresses of the Trap Managers to which Traps are to be sent.

3.3.4.2 WEB Configuration

1. Navigate to Administration→Network Configuration and click on the SNMP link in the left panel.
2. All SNMP related parameters are displayed with current/present values.
3. To revert to the previous values, press Reset button.
4. To change the parameters, enter new values and press “update” button.
5. The page will be refreshed and displayed with current/present values.
6. If parameters are not updated with entered values, the values entered may be invalid.
7. Values of **Read Community, Write Community, Trap Community, SNMP Auth Password, SNMP Priv Password** parameters will not be displayed because these parameters are treated as passwords.
8. if no values are entered for the parameters indicated above, the present values in the system will not be overwritten.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.4.3 CLI Configuration

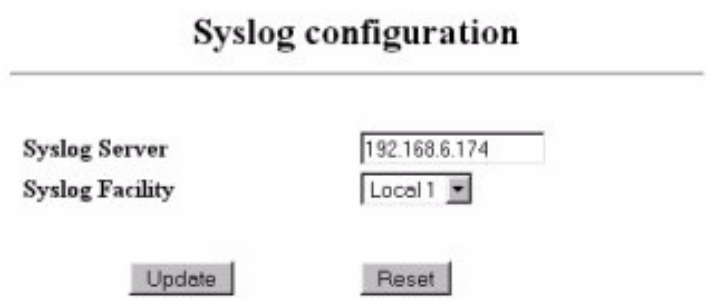
1. Navigate to Administration→ General Network Menu→ SNMP Configuration
2. All SNMP related parameters are displayed with current/present values.
3. To edit an individual parameter, enter its hotkey, edit its value and press the Enter key.
4. To revert to the previous value, press the “Esc” key while editing the value.
5. Scroll through the options for the following parameters using the Space Bar key and press the Enter key to select among the options.
   a. SNMP Mode
   b. Trap Version
   c. Auth Trap Enable
6. The page is refreshed and displayed with the updated or current/present values.
7. If parameters are not updated with entered values, the values entered may be invalid.

3.3.4.4 SNMP Configuration

1. Select a parameter from the MIB section SysCfgNetworkSNMP
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.5 Syslog Configuration



User Access Level:

User Access Level: Level 3

Figure 3.9. Syslog Configuration.

3.3.5.1 Description

Figure 3.9 shows the screen used to configure the following Syslog related parameters:

1. **Syslog IP** - Enter Syslog IP Address for the system. If unsure contact your network administrator.
2. **Syslog Facility** - Select Syslog facility for the system. If unsure contact your network administrator.

3.3.5.2 WEB Configuration

1. Navigate to Administration→Network Configuration→Syslog Configuration in the left panel.
2. All Syslog related parameters are displayed with current/present values.
3. To revert to previous values, press Reset button.
4. To change parameters, enter new values and press the “update” button.
5. The page is refreshed and displayed with the updated or current/present values.
6. If parameters are not updated with entered values, the values entered may be invalid for that parameter.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.5.3 CLI Configuration

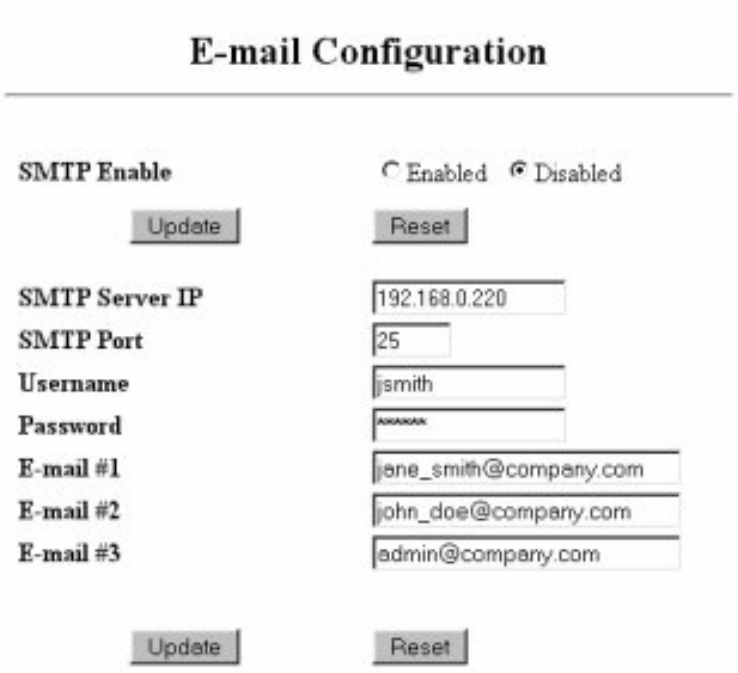
1. Navigate to Administration→General Network Menu→Syslog Configuration
2. All Syslog related parameters are displayed with current/present values.
3. To edit an individual parameter, enter its hotkey, edit its value and press the Enter key.
4. To revert to the previous value, press the “Esc” key while editing the value.
5. Scroll through the options for the following parameters using the Space Bar key and press the Enter key to select among the options.
    a. Syslog facility
6. To update the edited parameter, press the hotkey for “Update”.
7. The page is refreshed and displayed with the updated or current/present values.
8. If the parameters are not updated with the entered values, the values entered may be invalid for that parameter.

3.3.5.4 SNMP Configuration

1. Select a parameter from the MIB section SysCfgNetworkSysLog
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.6 E-mail Configuration



User Access Level: _____

User Access Level: Level 3

Figure 3.10. E-mail Configuration.

3.3.6.1 Description

The screen in Figure 3.10 is used to configure the following E-mail related parameters:

1. **SMTP Enable** – Enable / Disable mail.
2. **SMTP Server IP** – Enter the SMTP server IP. If unsure, contact your network administrator.
3. **SMTP Port** – Enter the SMTP port. Default 25.
4. **Username** – Enter the user name of your E-mail account.
5. **Password** – Enter the password of your mail account.
6. **E-mail #1 - #3** – Enter the recipients' mail addresses.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.6.2 WEB Configuration

1. Navigate to Administration→Network Configuration→E-mail Configuration in the left panel.
2. All E-mail related parameters are displayed with current/present values.
3. To revert to previous values, press Reset button.
4. To change the parameters, enter new values and press the “update” button.
5. The page is refreshed and displayed with the updated or current/present values.
6. If parameters are not updated with entered values, the value entered may be invalid for that parameter.

3.3.6.3 CLI Configuration

1. Navigate to Administration→General Network Menu→E-mail Configuration.
2. All E-mail related parameters are displayed with current/present values.
3. To edit an individual parameter, enter its hotkey, edit its value and press the Enter key.
4. To revert to the previous value, press the “Esc” key while editing the value.
5. Scroll through the options for the following parameters using the Space Bar key and press the Enter key to select among the options.
    a. SMTP Enable
6. To update the edited parameter, press the hotkey for “Update”.
7. The page is refreshed and displayed with the updated or current/present values.
8. If parameters are not updated with entered values, the value entered may be invalid for that parameter.

3.3.6.4 SNMP Configuration

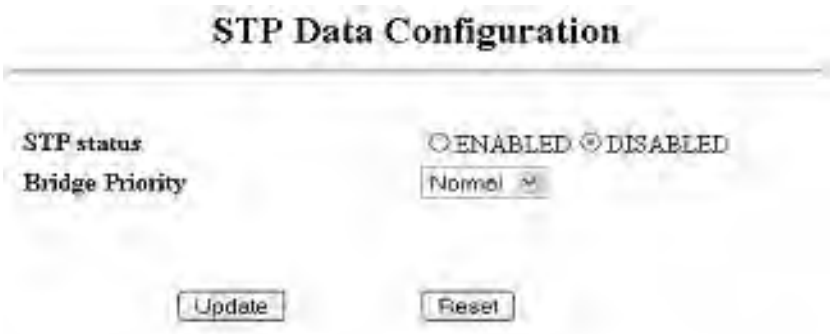
1. Select a parameter from the MIB section SysCfgNetworkEmail
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

Enable the “SMTP Enable parameter” to send e-mail to the specified addresses upon occurrence of selected alarms.

3.3.7 STP Data Configuration



User Access Level: **Level 3**

Figure 3.11. STP Data Configuration.

3.3.7.1 Description

This screen is used to configure the STP status (enable/disable) and the Bridge priority (see Figure 3.11).

3.3.7.2 WEB Configuration

1. Navigate to Administration→Network Configuration→STP Data in the left panel.
2. All STP Data parameters (STP Status and Bridge Priority) are displayed with current/present values.
3. To revert to previous values, press Reset button.
4. To change the parameters, enter new values and press the “update” button.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

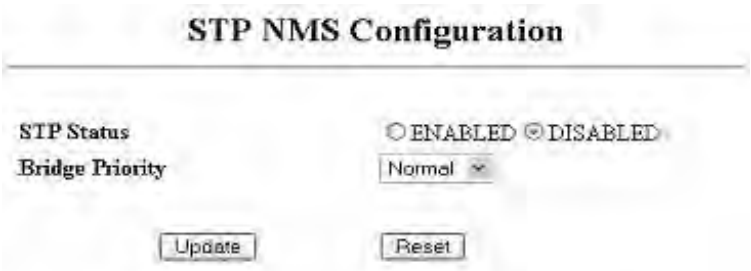
3.3.7.3 CLI Configuration

1. Navigate to Administration→ Network Configuration→ STP Configuration→Data Switch Configuration.
2. All STP Data parameters (STP Status and Bridge Priority) are displayed with current/present values.
3. To edit an individual parameter, enter its hotkey, modify its value by scrolling through the options using the Space Bar key.
4. To revert to the previous value, press the “Esc” key while editing the value.
5. To update the edited parameter, press the hotkey for “Update”.
6. The page is refreshed and displayed with the updated or current/present values.

3.3.7.4 SNMP Configuration

1. Select a parameter from the MIB section SysCfgNetworkSTPData
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

3.3.8 STP NMS Configuration



User Access Level:

User Access Level: Level 3

Figure 3.12. STP NMS Configuration.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.8.1 Description

This screen is used to configure STP NMS status (enable/disable) and Bridge priority (see Figure 3.12).

3.3.8.2 WEB Configuration

1. Navigate to and click on the Administration→Network Configuration→STP NMS.
2. All STP NMS parameters (STP Status and Bridge Priority) are displayed with current/present values.
3. To revert to previous value, press Reset button.
4. To change the parameters, enter new values and press the “update” button.

3.3.8.3 CLI Configuration

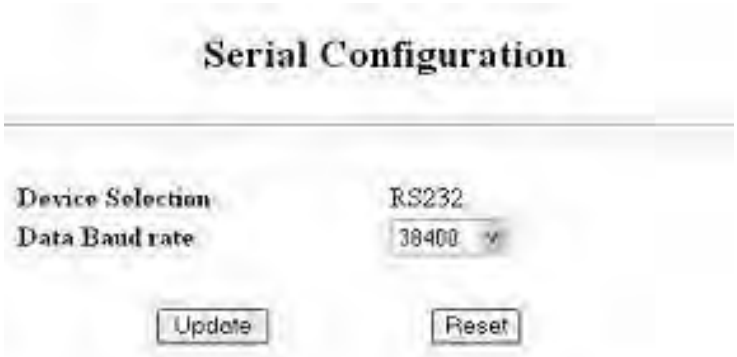
1. Navigate to Administration→ Network Configuration→ STP Configuration→ NMS Switch Configuration
2. All STP NMS parameters (STP Status and Bridge Priority) are displayed with current/present values.
3. To edit an individual parameter, enter its hotkey, modify its value by scrolling through the options using the Space Bar key, and press “Enter”.
4. To revert to the previous value, press the “Esc” key while editing the value.
5. To update the edited parameter, press the hotkey for “Update”.
6. The page is refreshed and displayed with the updated or current/present values.

3.3.8.4 SNMP Configuration

1. Select a parameter from the MIB section SysCfgNetworkSTPNMS
2. Use the SNMP GET command to get the value of the required parameter.
3. Use the SNMP SET command to set the value of the required parameter.
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.9 Serial Configuration



User Access Level: **Level 3**

Figure 3.13. Serial Configuration.

3.3.9.1 Description

The screen shown in Figure 3.13 is used to configure the following serial port related parameters.:

1. **Data Baud Rate** – Select the suitable baud rate for the selected device.

3.3.9.2 WEB Configuration

1. Navigate to Administration→Serial Configuration in the left panel.
2. All Serial port related parameters are displayed with current/present values.
3. To revert to previous values, press Reset button.
4. To change the parameters, enter new values and press the “update” button.
5. The page is refreshed and displayed with the updated or current/present values.
6. If parameters are not updated with entered values, the value entered may be invalid for that parameter.

3.3.9.3 CLI Configuration

1. Navigate to Administration→Serial Configuration

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

2. All Serial related parameters are displayed with current/present values.
3. To edit an individual parameter, enter its hotkey, edit its value and press the Enter key.
4. To revert to the previous value, press the “Esc” key while editing the value.
5. Scroll through the options for the following parameters using the Space Bar key and press the “Enter” key to select among the options.
   a. Device Selection
   b. Serial Byte Format
   c. Data Baud Rate
6. To update the edited parameter, press the hotkey for “Update”.
7. The page is refreshed and displayed with the updated or current/present values.
8. If parameters are not updated with entered values, the value entered may be invalid for that parameter.

The parameters like

1. PPPD Server IP
2. PPPD Client IP
3. PPPD Netmask

can be configured, only if the Device Selection parameter is set to “Modem With IP”

3.3.9.4 SNMP Configuration

1. Select a parameter from the MIB section SysCfgSerial
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.10 Device Information

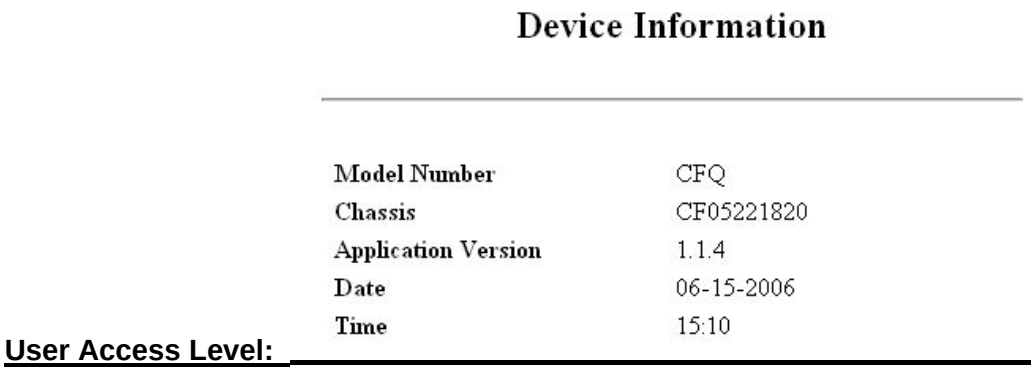


Figure 3.14. Device Information.

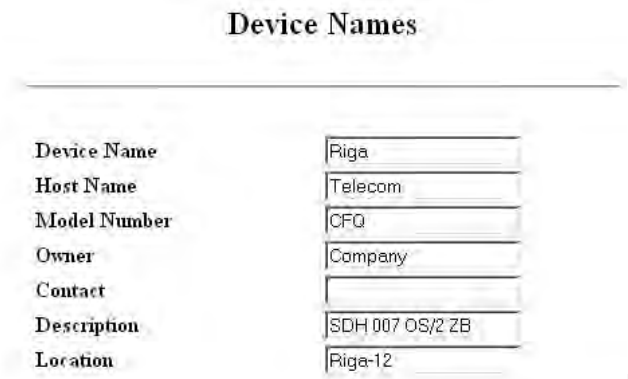
3.3.10.1 Description

The screen shown in Figure 3.14 is a read-only information page that provides the user with terminal related information. The parameters listed on this page are:

- **Model Number** – Model number of the terminal
- **Chassis Serial Number** – Chassis Serial Number assigned during manufacturing.
- **Application Version** – Active Application Version information.
- **Date** – Current Date.
- **Time** – Current Time.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.11 Device Names



User Access Level: **Level 3**

Figure 3.15. Device Names.

3.3.11.1 Description

This screen enables the user to modify terminal related information (see Figure 3.15). The parameters listed on this page are:

1. **Device Name** – Enter the name of the device.
2. **Host Name** – Enter the host name of the device.
3. **Model Number** – Enter the IDU model number.
4. **Owner** – Enter the name of the device owner.
5. **Contact** – Enter the contact information of owner.
6. **Description** – Enter the device description.
7. **Location** – Enter device location.

The Device Name and Owner values are displayed at the top of each CLI screen, as shown in Figure 3.16. The Device Name appears first and the Owner appears second. These parameters can be used to give a personalized appearance to the CLI.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

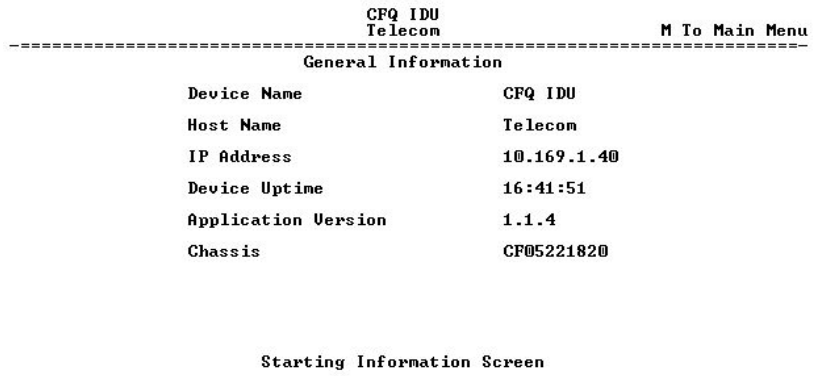


Figure 3.16. CLI Starting Information Screen

3.3.11.2 WEB Configuration

1. Navigate to Administration→Device Configuration and click on the “Device Names” link in the left panel.
2. The current values of the parameters are displayed here.
3. Select and modify desired parameters.
4. Click the “Update” to button submit these changes.
5. Click the “Reset” button to undo changes

3.3.11.3 CLI Configuration

1. Navigate to Administration→Device Configuration→Device Names
2. Device related parameters are displayed with current/present values.
3. To edit an individual parameter, enter its hotkey, edit its value and press the Enter key.
4. To revert to the previous value, press the “Esc” key while editing the value.
5. To update the edited parameter, press the hotkey for “Update”.
6. The page is refreshed and displayed with the updated or current/present values.
7. If parameters are not updated with entered values, the value entered may be invalid for that parameter.

3.3.11.4 SNMP Configuration

1. Select a parameter from the MIB section SysCfgDevInfoNames

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

3.3.12 Set Date and Time

User Access Level: **Level 3**

Figure 3.17. Set Date and Time.

3.3.12.1 Description

The screen shown in Figure 3.17 enables the user to modify the date and time of the terminal and set related parameters. The parameters listed on this page are:

1. **SNTP Server Enable** – Enable / Disable SNTP Client.
2. **SNTP Server Address** – Specify SNTP Server Address.
3. **Time Zone** – Specify time difference from GMT.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

4. **Date Format** – Specify desired date format (US, European, Generic)
5. **Date** – Set current terminal date.
6. **Time** – Set current terminal time.

3.3.12.2 WEB Configuration

1. Navigate to Administration→Device Configuration and click on the “Set Time and Date” link in the left panel.
2. The current values of parameters are displayed here.
3. Select and modify desired parameters.
4. Click the “Update” to button submit these changes.
5. Click the “Reset” button to undo changes

3.3.12.3 CLI Configuration

1. Navigate to Administration→Device Configuration→Date and Time
2. All Date and time related parameters are displayed with current/present values.
3. To edit an individual parameter, enter its hotkey, edit its value and press the Enter key.
4. To revert to the previous value, press the “Esc” key while editing the value.
5. Scroll through the options for the following parameters using the Space Bar key and press the Enter key to select among the options.
   a. Date Format
   b. SNTP Server Enable
6. To update the edited parameter, press the hotkey for “Update”.
7. The page is refreshed and displayed with the updated or current/present values.
8. If parameters are not updated with entered values, the value entered may be invalid for that parameter.

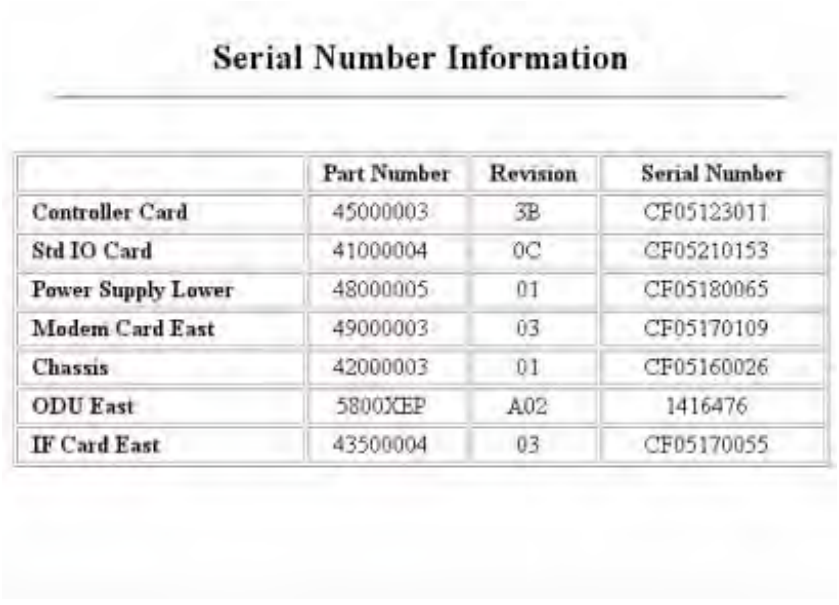
3.3.12.4 SNMP Configuration

1. Select a parameter from the MIB section SysCfgDevInfoDateTime
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

3.3.13 Serial Number Information



User Access Level:

User Access Level: Level 1

Figure 3.18. Serial Number Information.

3.3.13.1 Description

This screen provides Part number, Revision and serial number information of various cards (see Figure 3.18). The following cards numbers are displayed.

- Controller card, STD IO card, PS cards, Modem cards, IF cards, ODU and chassis.

3.3.13.2 WEB Configuration

1. Navigate to Administration→Device Information and click on the “Serial Numbers” link in the left panel.
2. The current values of various parameters are displayed here.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.13.3 CLI Configuration

1. Navigate to Administration→Device Configuration→Serial Number Information
2. All Serial Number related parameters are displayed with current/present values.
3. SNMP Configuration
4. Select a parameter from the MIB section SysCfgDevInfoCards
5. Use the SNMP GET command to get the value of the required parameter
6. The SNMP agent will return the actual value on successful get operation. Upon failure, the SNMP agent will return an error if agent is not able to get the value or the user does not have access rights to the selected parameter

3.3.14 Security Configuration

User Access Level: _____

User Access Level: Level 3

Figure 3.19. Security Configuration.

3.3.14.1 Description

The screen shown in Figure 3.19 enables the user to modify the security configuration of the terminal. The options listed on this page are:

1. **AES Encryption** – Enable / Disable AES Encryption.
2. **AES Encryption Phrase** – Specify the AES Encryption Phrase.
3. **HTTP** – Select Type of HTTP Access (SSL/None/Disabled).
4. **CLI** – Select Type of CLI Access (Telnet/ SSH / Disabled).

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.14.2 WEB Configuration

1. Navigate to Administration and click on the “Security Configuration” link in the left panel.
2. The current values of the parameters are displayed.
3. Select and modify desired parameters.
4. Click the “Update” to button submit these changes.
5. Click the “Reset” button to undo changes

3.3.14.3 CLI Configuration

1. Navigate to Administration→Security Configuration
2. All Security related parameters are displayed with current/present values.
3. To edit an individual parameter, enter its hotkey, edit its value and press the Enter key.
4. To revert to the previous value, press the “Esc” key while editing the value.
5. Scroll through the options for the following parameters using the Space Bar key and press the Enter key to select among the options.
   a. Command Line Interface
   b. HTTP Access
   c. AES Encryption
6. To update the edited parameter, press the hotkey for “Update”.
7. The page is refreshed and displayed with the updated or current/present values.
8. If parameters are not updated with entered values, the value entered may be invalid for that parameter.

3.3.14.4 SNMP Configuration

1. Select a parameter from the MIB section SysCfgSecurity
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.15 Reprogramming CPU

User Access Level: Level 3

Figure 3.20. Reprogramming.

3.3.15.1 Description

The screen shown in Figure 3.20 is used to Reprogram / Upgrade the terminal software remotely. SDIDU is built upon a modular software architecture, i.e. it is based on various software components, namely:

KERNEL – the operating system. It provides software application access to hardware. This component does not require frequent upgrades. Kernel upgrade is not necessary in case of performing minor upgrades.

APPLICATION - the set of software applications that the system runs: set of programs that perform functions like Web GUI, Link Configuration and process monitoring. This component changes when new features are introduced. It is usually a part of software upgrade and must match the ODU library version.

FPGA – software intended for the devices controlling data flow through the system. All the images for these devices are packed into one fpga.img. This software is updated independently with its own set of software improvements or with a major software release supporting new types of data traffic.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

ODU – software component that ensures application interface with a specific type of ODU. It is different for each Application version, so corresponding software should be used for a particular upgrade.

MODES – software file containing various modes that can be configured by a user. Modes combine different RF bandwidths and modulation types with the types of data traffic to be sent over the RF link. This file is updated to add or subtract new modes.

CHANNELS – file containing various channels displayed for user to choose between them in order to perform configuration. This file is updated to add or subtract these channels.

ODU EAST/WEST FIRMWARE – file intended for the upgrade of ODU internal micro-controller that runs a specific program. ODU East or West Firmware refers to the firmware (software program) used in the ODU that is attached to the corresponding East or West SDIDU Modem. It is upgraded when the ODU has an upgraded firmware available.

BOOTLOADER – the initial program that is run at system power-up, which loads the Operation System, Application and other software into memory and runs it. It does not change often, and therefore upgrade is necessary only on rare occasions.

MODEM EAST /WEST FIRMWARE – file intended for the upgrade of the internal controller of modem card. It is updated independently from the Application. The upgrade is necessary in case of design improvement or changes aimed to support new features made available in the ODU library.

This page (Figure 3.20) enables the user to upgrade the Kernel, Application, FPGA, ODU, modes, channel, Boot Loader, ODU and Modem firmware Images. The options available are listed below. Some options are only available depending on the type of upgrade.

1. **Image Type** – To Select File type that is going to be transferred.
2. **Toggle Image button** – Will swap the Active and Passive files, i.e. active file will become passive and vice versa.
3. **Version Information** – Will display the version information for both active and passive images. The active/Working image will be indicated by .

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.16 WEB Configuration

1. Navigate to Administration→Maintenance→reprogramming screen.
2. Select an Image type.
3. To toggle between images, press the toggle button.
4. In the event of an error, an appropriate error message will be displayed.

3.3.16.1 CLI Configuration

1. Navigate to Administration→Maintenance→reprogramming CPU screen.
2. Scroll through the file names using the Space Bar key and press the Enter key to select one. Wait for few seconds to allow the screen refresh.
3. To toggle between images,
   a. press the hotkey for toggle.
   b. The result will be displayed on the screen.
   c. In the event of an error, an appropriate error message will be displayed.

3.3.16.2 SNMP Configuration

1. Select a parameter from the MIB section SysCfgMaintenanceReprog
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

RpgServerIP, RpgFiletype and RpgTftpTimeout parameters must be set before performing any reprogramming operations.

A reboot is required after toggle of kernel, applications, FPGA, or ODU.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.17 Add User Entry:

User Access Level:

User Access Level: Level 3

Figure 3.21. Add User.

3.3.17.1 Description

This screen enables the administrators of the terminal to add users to the terminal (see Figure 3.21). The options listed on this page are:

1. **User ID** – Username.
2. **Group ID / Level** – Specify access level
3. **Password** – Password for the entered user id.
4. **Confirm** – Confirm Password entered.

Administrators may not add users with an access level greater than their own.

3.3.17.2 WEB Configuration

1. Navigate to Administration→Maintenance and click on the “Add User” link in the left panel.
2. Edit fields.
3. Click the “Add” button add a new user.
4. Click the “Reset” button to reset page.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.17.3 CLI Configuration

1. Navigate to Administration→Maintenance→User Management→Add User.
2. Edit each parameter.
3. Scroll through the options for the Level parameter using the Space Bar key and press the Enter key to select one.
4. Press the hotkey for “Update” to add new user.

3.3.17.4 SNMP Configuration

1. Select a parameter from the MIB section SysCfgMaintenanceUserMgmt
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

The SNMP agent allows a maximum of 5 users. By default, the user name “admin” with level 4 access rights will be present. The “admin” user’s passwords can be changed from the CLI or WEB interfaces only.

New users can be added in SNMP v3 mode.

The Web and CLI interfaces restrict the maximum number of users to 10. If 10 users exist, an error message will be displayed. Delete an existing user to add new user.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.18 Delete / Edit User Entry

User Access Level: _____

User Access Level: Level 3

Figure 3.22. Delete User.

3.3.18.1 Description

The screen shown in Figure 3.22 enables the administrators of a terminal to remove users from the terminal. The page also allows a user to change the password of any user whose access level is less than or equal to his own.

1. **Delete User** – Username of user to be removed.
2. **Change Password** – Change Password of the selected User.

A user can change his own password and the passwords of users whose access level is equal or less than his own level.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.18.2 CLI Configuration

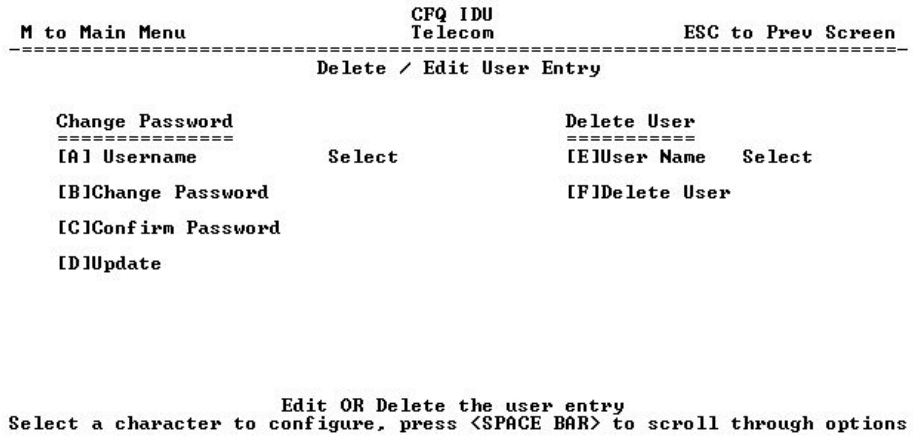


Figure 3.23. Delete/Edit User Entry.

Figure 3.23 shows the CLI version of the Delete/Edit User Entry screen. The options listed on this page are:

1. **Username** – Select the username to change his password
2. **Change Password –** Enter the new password for the selected user
3. **Confirm Password –** Confirm the new password
4. **Update –** Update the change in password in selected user profile.
5. **Username** – Select the username to remove his entry
6. **Delete User** – Delete the selected user

To use this screen:

1. Navigate to Administration→Maintenance→User Management→Edit/Delete User Entry.
2. To change the password, select the username and enter new password, confirm the entered password and press the hotkey to Update new password.
3. To delete a user, select the username and press the hotkey for Delete User.

3.3.18.3 WEB Configuration

1. Navigate to Administration→Maintenance and click on the “Del User” link in the left panel.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

2. Select the user to be removed from the drop down menu.
3. Click the “Delete” button to remove the user from the terminal.

3.3.18.4 SNMP Configuration

1. Select a parameter from the MIB section SysCfgMaintenanceUserMgmt
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

The default “admin” user cannot be deleted.

To change the password for a particular user, the user will have to be removed from the terminal and added again

3.3.19 View Event Log

Figure 3.24. Eventlog.

3.3.19.1 Description

This screen shown in Figure 3.24 enables the administrators of a terminal to view the event log of the terminal and clear it when required. A log of terminal access is available here in the form of a table listing user and time of login. This log is

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

non-volatile and available across terminal reboots. Pressing the “clear” button clears the event log.

To access the event log from SNMP go to the MIB section SysCfgMaintenanceEventLog

To clear the event log from SNMP go to the MIB section SysCfgMaintenanceEventLog, and SET the MIB ClearEventLog.

3.3.20 Restore System Defaults

User Access Level:

User Access Level: Level 3

Figure 3.25. Restore System Defaults.

3.3.20.1 Description

The screen shown in Figure 3.25 enables the user to restore all terminal defaults.

3.3.20.2 WEB Configuration

To restore the terminal defaults, click the “restore” button.

3.3.20.3 CLI Configuration

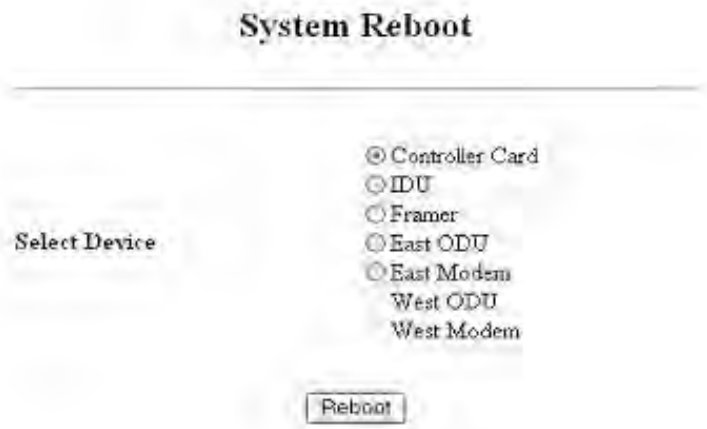
1. Navigate to Restore Defaults screen.
2. Press the hotkey for “Restore Defaults”.
3. When asked for confirmation, press “y” to proceed or “n” to cancel.
4. A success or failure message will be displayed.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.20.4 SNMP Configuration

1. Select a parameter from the MIB section SysCfgCmd
2. Use the SNMP SET command to set the value of the RestoreDefaults MIB object
3. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

3.3.21 System Reboot



User Access Level:

User Access Level: Level 2

Figure 3.26. System Reboot.

3.3.21.1 Description

The screen shown in Figure 3.26 enables the user to reboot the terminal or certain devices within the terminal.

It will display a list of devices and the user can select a device depending on the availability and configuration of devices.

3.3.21.2 WEB Configuration

1. Select the device to reboot from the list.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

2. Click “reboot” button.

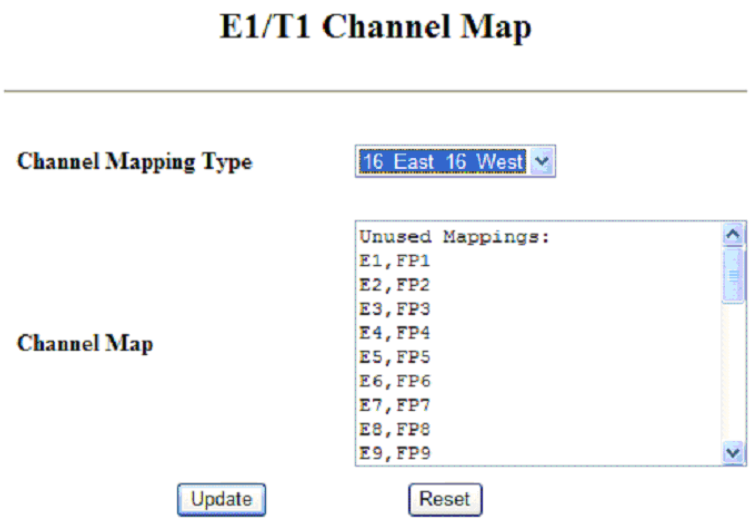
3.3.21.3 CLI Configuration

1. Navigate to System Screen
2. Select the Device to reboot using the Space Bar key and press the Enter key to select.
3. Press the hotkey for “Reboot”.
4. When asked for confirmation, press “y” to proceed or “n” to cancel.
5. A success or failure message will be displayed.

3.3.21.4 SNMP Configuration

1. Select a parameter from the MIB section *SysCfgCmd*
2. Use the SNMP SET command to set the value of the Reboot MIB object
3. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

3.3.22 E1 / T1 Channel Map



User Access Level: **Level 2**

Figure 3.27. E1/T1 Channel Map

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.22.1 Description

This page enables the user to modify the E1 / T1 channel map settings (see Figure 3.27. E1/T1 Channel Map).

The following are displayed:

1. **Front panel port x** – To select/map a timeslot to this front panel port.
2. **Pass through x** (only in East-West Mode) – To select/map a timeslot for pass through operation.

3.3.22.2 WEB Configuration

1. Navigate to Data Link and click on the “E1/T1 Channel Map” link in the left panel.
2. The current values of the channel map are displayed.
3. Map desired timeslots to front panel ports.
4. Click the “Update” button to submit these changes.
5. Before updating the values in the system, the user interface performs a validation to detect incorrect mapping. In case of failure, an error message with the location of the error will be displayed. Before pressing update, take care of the following conditions to avoid error.
    a. Map all available timeslots.
    b. Do not map a timeslot more than once.
    c. Do not map a front panel port to both an east and a west timeslot.
    d. For pass-through, map any timeslot in both east and west.

3.3.22.3 CLI Configuration

1. Navigate to Link Configuration→Data Links→E1/T1 Ports→E1/T1 Channel Map.
2. The current values of the channel map are displayed.
3. Map desired timeslots to front panel ports.
4. Click the “Update” button to submit these changes.
5. Before updating the values in the system, the user interface performs a validation to detect incorrect mapping. In case of failure, an error message with the location of the error will be displayed. Before pressing update, take care of the following conditions to avoid error.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

6. Map all available timeslots.
   a. Do not map a timeslot more than once.
   b. Do not map a front panel port to both east and west timeslot.
   c. For pass-through, map any timeslot in both east and west.

3.3.22.4 SNMP Configuration

1. Select a parameter from the MIB section LinkCfgDataE1T1Ports
2. Use DataE1T1EastChMapFrontPanelTable, DataE1T1EastChMapPassThruTable, DataE1T1WestChMapFrontPanelTable and DataE1T1WestChMapPassThruTable MIB sections to select the channel mapping
3. Use E1T1ChMapReconfigure MIB variable to update the selected channel map
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.23 E1 / T1 Ports

User Access Level: Level 2

Figure 3.28. E1/T1 Configurations

3.3.23.1 Description

This screen enables the user to configure the following E1 / T1 channel related parameters (see Figure 3.28):

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

1. **Channel section Checkbox** – To select channel(s) to apply configurations.
2. **Encoding** – To select encoding for selected E1 / T1 channel.
3. **TX Data** – To select TX data for selected E1 / T1 channel.
4. **Loop back** – To select Loop back for selected E1 / T1 channel.
5. **LOS Action** – To select LOS Action for selected E1 / T1 channel. “Auto transmit all ones” will be selectable only if TX Data is “All ones”.
6. **AIS type** – To select AIS type for selected E1 / T1 channel. Depending on the channel type (E1 / T1) configuration, the choices displayed will differ.
7. **Build out** – To select Build out for selected E1 / T1 channel. Depending on the channel type (E1 / T1) configuration, the choices displayed will differ.

3.3.23.2 WEB Configuration

1. Navigate to Link Configuration→Data Link and click on the “E1/T1 Ports” link in the left panel.
2. All configured channels will be displayed with their current configurations in the form of table.
3. To configure channel(s), click on that channel’s checkbox.
4. Change the required parameters under “new settings” and click “update” button.

3.3.23.3 CLI Configuration

The CLI uses two screens to configure the E1 /T1 channel related parameters.

3.3.23.3.1 E1 / T1 Active Channel Screen:

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

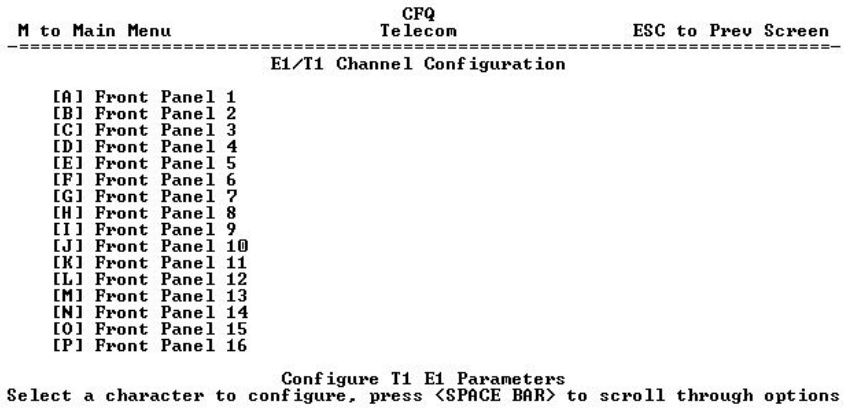

CFQ
M to Main Menu
Telecom
ESC to Prev Screen
E1/T1 Channel Configuration
[A] Front Panel 1
[B] Front Panel 2
[C] Front Panel 3
[D] Front Panel 4
[E] Front Panel 5
[F] Front Panel 6
[G] Front Panel 7
[H] Front Panel 8
[I] Front Panel 9
[J] Front Panel 10
[K] Front Panel 11
[L] Front Panel 12
[M] Front Panel 13
[N] Front Panel 14
[O] Front Panel 15
[P] Front Panel 16
Configure T1 E1 Parameters
Select a character to configure, press <SPACE BAR> to scroll through options

Figure 3.29. T1/E1 Active Channels

To use the screen shown in Figure 3.29. T1/E1 Active Channels

1. Navigate to IDU Configuration→Data Link Configuration→E1/T1 Ports→E1/T1 Channels Configuration
2. Press hotkey corresponding to the E1/T1 channel to configure (see Figure 3.29. T1/E1 Active Channels).
3. Upon pressing the hot key, the screen shown in Figure 3.30. T1/E1 Channel Configuration will be displayed.

3.3.23.3.2 E1 / T1 Configuration Screen

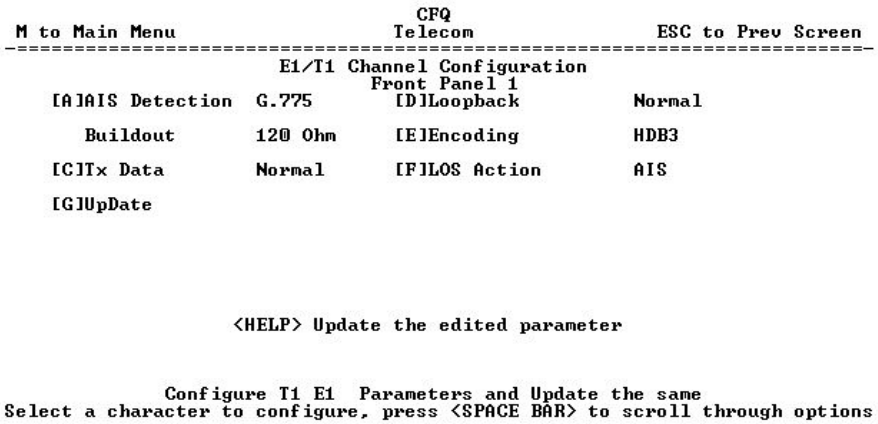


Figure 3.30. T1/E1 Channel Configuration

1. On the T1 E1 Channel Configuration screen (Figure 3.30. T1/E1 Channel Configuration), all E1 T1 parameters are displayed with current/present values.
2. To edit an individual parameter, enter its hotkey, edit its value and press the Enter key.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

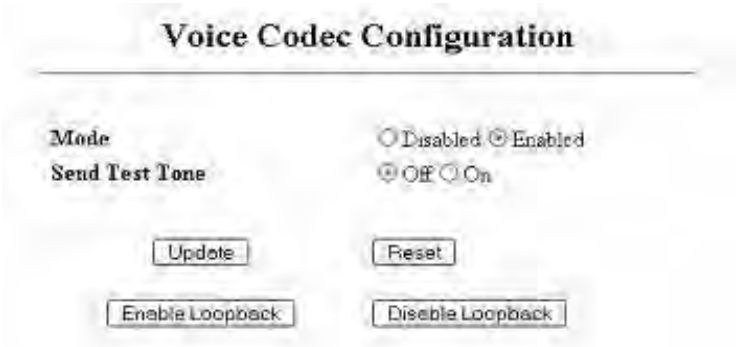
3. To revert to the previous value, press the “Esc” key while editing the value.
4. Scroll through the options of all the E1 / T1 parameters using the Space Bar key and press the Enter key to select among the options.
5. To update the edited parameter, press the hotkey for “Update”.
6. The page is refreshed and the updated or current/present values are displayed.
7. If parameters are not updated with entered values, the value entered may be invalid for that parameter.

3.3.23.4 SNMP Configuration

1. Select a parameter from the MIB section LinkCfgDataE1T1Ports
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

To configure E1 / T1 related parameters, the Standard IO card should be configured and present. Otherwise an error message will be displayed.

3.3.24 Voice Code



User Access Level: **Level 3**

Figure 3.31. Voice Codec Configuration

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.24.1 Description

The screen shown in Figure 3.31 enables the user to configure the following voice codec channel related parameters.

1. **Mode** – To Enable/Disable voice codec mode.
2. **Send test tone** – To send test tone (On/Off).
3. **Enable Loopback** – To Enable loopback
4. **Disable Loopback** – To Disable loopback

3.3.24.2 WEB Configuration

1. Navigate to Link Configuration→Data Link and click on the “Voice codec” link in the left panel.
2. Voice codec related parameters will be displayed with current/present value.
3. If Loopback is required click the “Enable Loopback” button.
4. If Loopback has to be disabled press the button “Disable loopback”.
5. Change the required parameters and click “update” button.

3.3.24.3 CLI Configuration

1. Navigate to IDU Configuration→Data Link Configuration→Voice Codec Configuration.
2. All Voice Codec parameters are displayed with current/present values.
3. To edit an individual parameter, enter its hotkey, edit its value and press the Enter key.
4. To revert to the previous value, press the “Esc” key while editing the value.
5. Scroll through the options of all the Voice Codec parameters using the Space Bar key and press the Enter key to select among the options.
6. To update the edited parameter, press the hotkey for “Update”.
7. The page is refreshed and displayed with the updated or current/present values.
8. If parameters are not updated with entered values, the value entered may be invalid for that parameter.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.24.4 SNMP Configuration

1. Select a parameter from the MIB section LinkCfgDataVoiceCodec
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

To configure Voice codec related parameters, the Standard IO card should be configured and present. Otherwise an error message will be displayed.

3.3.25 STM1/OC3 Channel Map

User Access Level:

User Access Level: Level 2

Figure 3.32. STM-1/OC-3 Channel Map

3.3.25.1 Description

Contact SAF Tehnika for availability.

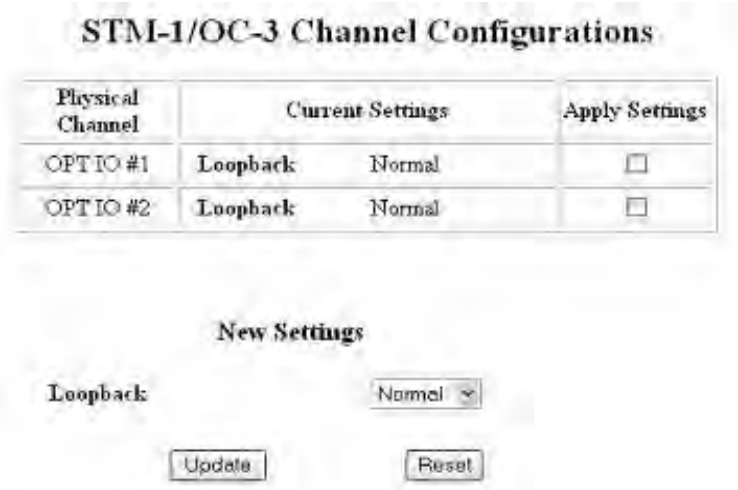
The screen shown in Figure 3.32 enables the user to modify the channel map settings of STM1/OC3.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.25.2 WEB Configuration

1. Navigate to Data Link and click on the “STM1/OC3 Channel Map” link in the left panel.
2. The current values of the channel map are displayed.
3. Select and modify the desired channel numbers.
4. Click the “Update” button to submit these changes.
5. Click the “Reset” button to undo changes.

3.3.26 STM1/OC3 Ports



User Access Level: **Level 2**

Figure 3.33. STM-1/OC-3 Channel Configurations

3.3.26.1 Description

Contact factory for availability.

The screen shown in Figure 3.33 enables the user to configure the following STM-1 channel related parameters.

1. **Channel Selection check box** – To select STM-1 Channel(s).
2. **Loop back** – To select Loop back (Normal, Local, Remote).

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.26.2 WEB Configuration

1. Navigate to Link Configuration→Data Link and click on the “STM1/OC3 Ports” link in the left panel.
2. All configured channels will be displayed with their current settings.
3. To configure channel(s), check the checkbox(es) next to that channel number(s).
4. Change the required parameters under “New settings” and click the “update” button.

3.3.26.3 CLI Configuration

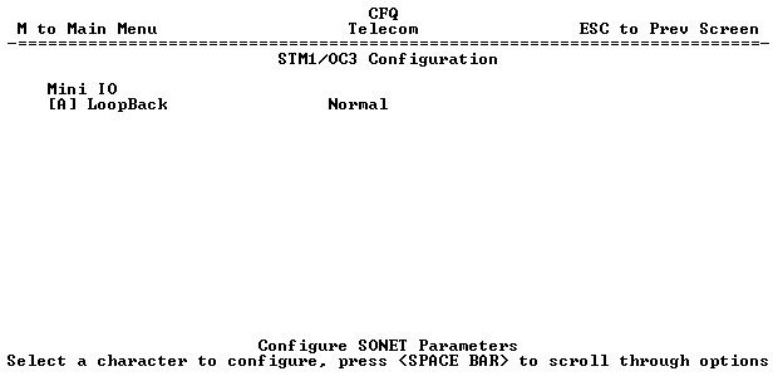


Figure 3.34. STM1/OC3 Configuration

1. Navigate to IDU Configuration→Data Link Configuration→STM1/OC3 Configuration.
2. All STM-1 parameters are displayed with current/present values (see Figure 3.34. STM1/OC3 Configuration).
3. To revert to the previous value, press the “Esc” key while editing the value.
4. Scroll through the options of all the STM-1 parameters using the Space Bar key and press the Enter key to select among the options.
5. The page is refreshed and displayed with the updated or current/present values.
6. If parameters are not updated with entered values, the value entered may be invalid for that parameter.

3.3.26.4 SNMP Configuration

1. Select a parameter from the MIB section LinkCfgDataSTM1OC3Ports

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

To configure STM-1 related parameters, the Optional IO and/or the Mini IO card should be configured and present. Otherwise an error message will be displayed.

3.3.27 Authorization

User Access Level: Level 3

Figure 3.35. Authorization Key

3.3.27.1 Description

The screen shown in Figure 3.35 enables the user to enter an authorization key.

3.3.27.2 WEB Configuration

1. Navigate to Link Configuration and click on the “Authorization” link in the left panel.
2. Enter the authorization key and press “Update”.
3. If the entered authorization key is valid, “Key accepted” is displayed. Otherwise “Invalid Key” is displayed.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.27.3 CLI Configuration

1. Navigate to IDU Configuration→Radio Link→ACR Key
2. To edit ACR, enter its hotkey, enter ACR phrase and press the Enter key.
3. If the entered authorization key is valid, “Valid ACR Key” is displayed. Otherwise, “Invalid ACR Key” is displayed.

3.3.27.4 SNMP Configuration

1. Select a parameter from the MIB section LinkCfgAuthorization
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

3.3.28 Configuration Summary

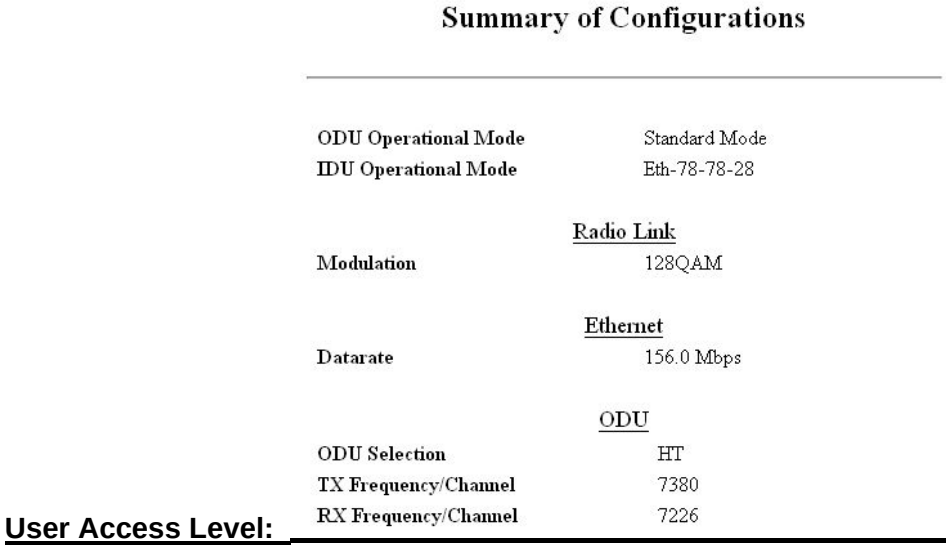


Figure 3.36. Summary of Configurations

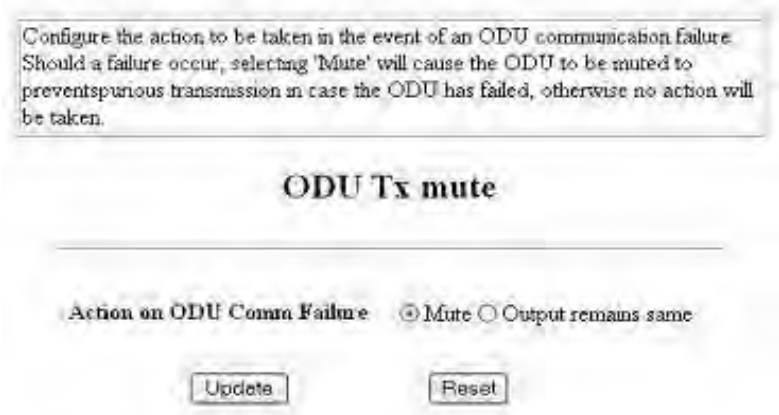
The screen shown in Figure 3.36 displays the current/present value of Framer and ODU parameters. In the case of East-West mode of operation, parameters will be displayed in two columns.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

The parameters displayed are:

1. ODU operation mode
2. IDU mode
3. E1 / T1 mode
4. E1 / T1 number of active channels
5. E1 / T1 active channel list
6. STM-1 number of active channels (Contact factory for availability)
7. STM-1 active channel list (Contact factory for availability)
8. ODU type (LT: Low-band transmit, HT: high-band transmit)
9. ODU polarization (horizontal, vertical: if supported)
10. ODU channel number

3.3.29 Tx Mute Configuration


Configure the action to be taken in the event of an ODU communication failure. Should a failure occur, selecting 'Mute' will cause the ODU to be muted to preventspurious transmission in case the ODU has failed, otherwise no action will be taken.
ODU Tx mute
Action on ODU Comm Failure
Mute
Output remains same
Update
Reset

User Access Level:

User Access Level: Level 3

Figure 3.37. ODU Tx mute

3.3.29.1 Description

This screen enables the user to configure the ODU Tx mute parameter (see Figure 3.37). This page will not be available in the case of protected (1+1) operation.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

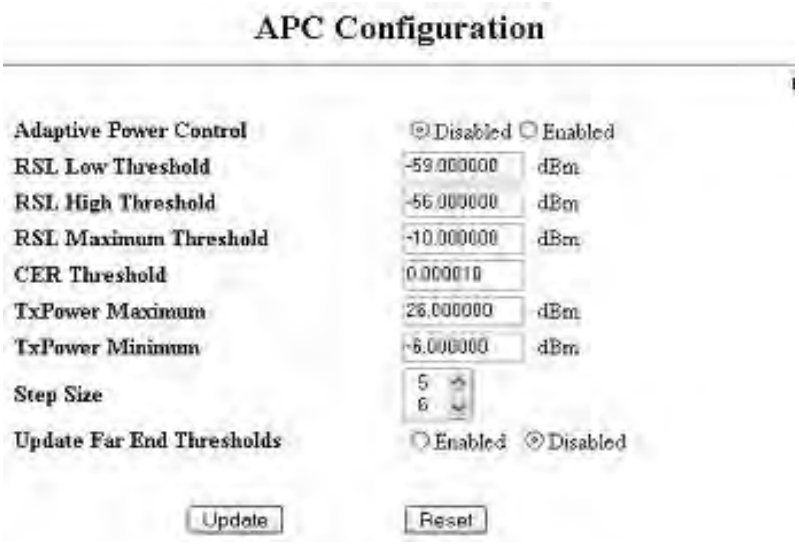
3.3.29.2 WEB Configuration

1. Navigate to Link Configuration→Radio Link and click on the “ODU Tx Mute Configuration” link in the left panel
2. Click on the radio button to select the required option and click the “update” button.

3.3.29.3 SNMP Configuration

1. Select a parameter from the MIB section LinkCfgRadioLinkProtection-> RadioLinkProtTxMuteCfg
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

3.3.30 APC Configuration



User Access Level: **Level 3**

Figure 3.38. APC Configuration

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.30.1 Description

This screen enables the user to configure the following APC parameters (see Figure 3.38).

1. **APC** - to enable or disable
2. **RSL Low Threshold** - current value is displayed
3. **RSL High Threshold** - current value is displayed
4. **RSL Maximum Threshold** - current value is displayed
5. **CER Threshold** - current value is displayed
6. **Tx Power Maximum** - current value is displayed
7. **Tx Power Minimum** - current value is displayed

3.3.30.2 WEB Configuration

1. Navigate to Link Configuration and click on the “APC Configuration” link in the left panel.
2. To enable/disable APC, click on the radio button and click the “update” button.
3. To change RSL Low Threshold, RSL High Threshold, RSL Maximum Threshold, CER Threshold, Tx Power Minimum, and Tx Power Maximum values or Step size, enter required value in the text box (for Step Size scroll through the select box) and click “update” button.
4. To Enable/Disable “Update Far End Thresholds” parameter, select the required radio button and press “Update” button.

3.3.30.3 SNMP Configuration

1. Select a parameter from the MIB section LinkCfgRadioLinkAPC
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP GET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if value is set our of range, or the agent is not able to get or set the value or the user does not have access rights to the selected parameter

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.31 Protection Configuration

User Access Level:

User Access Level: Level 3

Figure 3.39. Protection Configuration

3.3.31.1 Description

This screen enables the user to configure the following protection parameters (see Figure 3.39).

1. **RSL Minimum Threshold** and **SNR Minimum Threshold** – Displays current values of these parameters.
2. **TX Switch on ODU Communication Failure**.
3. **Power down ODU after switch** – Enable/Disable querying the faulted ODU for its status.
4. **Switch Transmitting ODU** (only in protected 1+1 mode).
5. **Preferred ODU selection** (only in protected 1+1 mode).

3.3.31.2 WEB Configuration

1. To change RSL Minimum threshold and SNR Minimum Threshold values, enter required value in the text box and click “update” button.
2. To Enable/Disable “**TX Switch on ODU Communication Failure**” parameter, select the required radio button and press “**Update**” button.
3. To Enable/Disable “**Power down ODU after switch**” parameter, select the required radio button and press “Update” button.
4. To switch the transmitting ODU (only in protected 1+1 mode), press the “**Switch Transmitting ODU**” button.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

5. To select a preferred ODU (only in protected 1+1 mode), click on the radio button (East/West) and press the “update” button.

3.3.31.3 SNMP Configuration

1. Select a parameter from the MIB section LinkCfgRadioLinkProtection
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP GET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if value is set our of range, or the agent is not able to get or set the value or the user does not have access rights to the selected parameter

3.3.32 Link Configuration Wizard

User Access Level: _____

User Access Level: Level 2

Figure 3.40. Link Configuration Wizard

3.3.32.1 Link Wizard Description

This screen enables the user to configure Framer and ODU related parameters.

The entire Framer and ODU configuration is divided across many pages, the first of which is shown in Figure 3.40. The pages are:

1. ODU op-mode page – To select ODU operation mode.
2. IDU op-mode page – To select IDU operation mode.
3. ODU configuration page – To configure ODU type, polarization, alignment mode and starting TX power.
4. ODU channel plan page – To select channel number for ODU.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

5. Summary page – Displays all parameter values as selected by the user from the proceeding pages. Upon pressing the “update” button, all Framer and ODU parameters are updated.

1. A single set of Framer and ODU parameters will be displayed for the “standard” ODU operational mode.
2. A single set of Framer parameters and two sets of ODU parameters will be displayed for the “Protected” ODU op-mode.
3. Two sets of Framer and ODU parameters will be displayed, if the ODU op-mode selected on the first page of the wizard is “East-West”.

3.3.32.2 WEB Configuration

1. Navigate to and click on the “Link configuration” link in the left panel.
2. Select ODU op-mode and click the “next” button.
3. Select IDU op-mode and click the “next” button. In the case of East-West mode, two independent IDU op-modes can be selected.
4. Select ODU type, Polarization, and Alignment Mode. Enter Starting TX Power and press the “next” button.
5. Select/Enter ODU Channel Number and press the “next” button.
6. All the above selected parameters are displayed the summary page. Verify all values and press the “update” button. To reconfigure, click the “redo” button in summary page.
7. After pressing the “Update” button, a new page will display the status of link configuration.

To configure the Framer and ODU related parameters, a standard IO card and modem should be configured and present. Otherwise an error message will be displayed.

In the Link Configuration Wizard, use only “back”/ “next” button given in the web page to move to previous/next page. **Do not use the browser back button**.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

If the selected parameters on the current page are not supported by the terminal, an error message will be displayed on the next page. To correct the error, go back to the previous page and select a different value for that parameter.

3.3.32.3 CLI Configuration

1. Navigate to IDU Configuration→Radio Link→Radio Wizard→ODU opmode Screen
2. Select ODU op-mode using the Space Bar key and press the Enter key. Then press the hotkey to switch to the Framer IDU operation mode Selection Screen.
3. Select IDU op-mode using the Space Bar key and press the Enter key. In the case of East-West mode, two independent IDU op-modes can be selected.
4. Select the ODU type, Polarization and Alignment Mode using the Space Bar key and press the Enter key. Enter the Starting TX Power. Then, press the hotkey to switch to ODU East Channel Selection Screen
5. Select ODU East Channel Number using the Space Bar key and press the Enter key. Then, press the hotkey to switch to the Reconfigure Framer Screen
6. If the ODU Opmode is East-West, then the user can select the ODU West channel number by switching to the ODU West Channel Selection Screen.
7. The selected parameters will be displayed in the summary page. Verify all values. To update, press the hotkey for “Update IDU Config Params”. To reconfigure, press the hotkey for “Radio Wizard – ODU opmode Selection”.

To configure the Framer and ODU related parameters, a standard IO card and modem should be configured and present. Otherwise an error message will be displayed.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

If the selected parameters in the current screen are not supported by the system, an error message will be displayed on the next page. Go back to the previous screen by pressing the Esc key and select a suitable value for that parameter.

3.3.32.4 SNMP Configuration

1. Select a parameter from the MIB section LinkCfgRadioLink
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

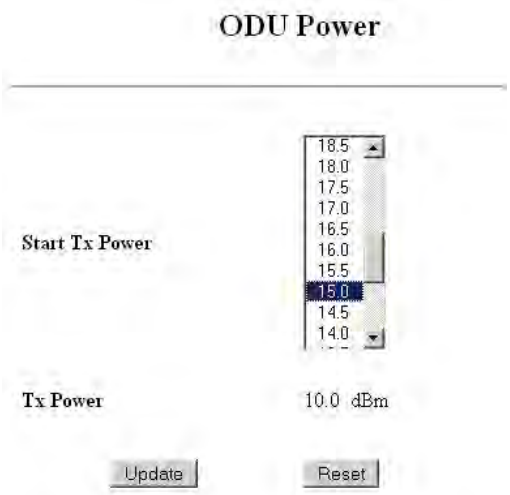
Wizard-style action in SNMP is achieved by setting a MIB object “LinkCfgMode”. If this MIB object is enabled then the entire Link configuration will be updated into the temporary wizard section. After the full configuration, the “RadioLinkReconfigure” MIB object needs to be set to reflect the changes made.

A detailed procedure for link configuration through SNMP is listed below

1. SET the ODU Opmode by setting the “LinkCfgODUOpMode” MIB object.
2. GET the IDU opmode list by reading the MIB “LinkUtilIDUEastOpmodeList”. “List” will give the list of possible op modes. Select a number corresponding to the required opmode.
3. SET IDU op-mode by setting the number selected above in to MIB object “LinkEastOpModeIndex”
4. GET the “LinkUtilEastODUChList” MIB variables value
5. SET the channel number gotten above in to the “RadioEastODUCfgChFreq”.
6. Update the configurations done so far using “RadioLinkReconfigure”
7. The selected configuration row index can be viewed by reading the MIB “LinkUtilEastChRowIndex”

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.33 ODU Power



User Access Level:

User Access Level: Level 2

Figure 3.41. ODU Power

3.3.33.1 Description

The screen shown in Figure 3.41 enables the user to configure the ODU power.

The following parameters are displayed

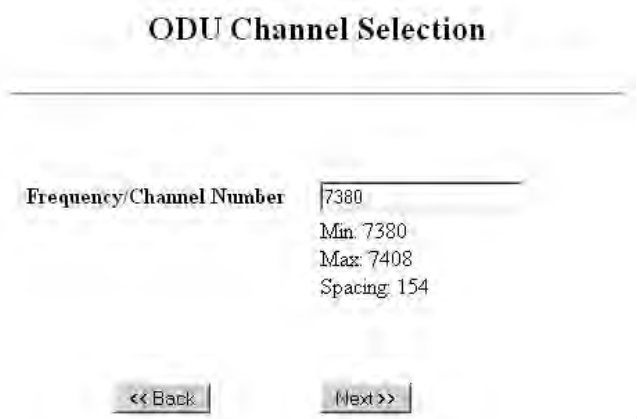
1. **Start Tx Power** - To change the starting Tx power of ODU.
2. **Current Tx Power** – To display the current Tx power.

3.3.33.2 WEB Configuration

1. Select the required Start Tx Power by pressing the UP or DOWN arrows and click the “update” button.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.34 ODU Channel selection



User Access Level: **Level 2**

Figure 3.42. ODU Channel

3.3.34.1 ODU Wizard Description

This screen enables the user to configure ODU related parameters. The ODU configuration is divided into many pages, the first of which is shown in Figure 3.42. The pages are:

1. ODU Configuration page – To configure ODU type, polarization and alignment mode.
2. ODU Channel Plan page – To select the channel number for ODU.

A single set of ODU parameters will be displayed for the “standard” ODU op-mode.

Two sets of ODU parameters will be displayed for the “Protected” and “East-West” ODU op-modes.

3.3.34.2 WEB Configuration

1. Navigate to and click on the “ODU configuration” link in the left panel.
2. Select the ODU type, polarization and alignment mode. Then press the “next” button.
3. Select the ODU channel number and press the “next”/ “update” button.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

To configure ODU related parameters, a modem should be configured and present. Otherwise an error message will be displayed.

In the Link Configuration Wizard, use only “back”/ “next” button given in the web page to move to previous/next page. **Do not use the browser back button**.

If the selected parameters on the current page are not supported by the terminal, an error message will be displayed on the next page. To correct the error, go back to the previous page and select a different value for that parameter.

3.3.34.3 CLI Configuration

1. Navigate to IDU Configuration→Radio Link→IDU ODU Configuration→ODU Configuration.
2. Select the ODU type, polarization and alignment mode using the Space Bar key and press the Enter key. Enter the starting TX power and press the hotkey to switch to the ODU Channel selection screen.
3. Select the ODU channel number and press the hotkey for “update.”

To configure ODU related parameters, a modem should be configured and present. Otherwise an error message will be displayed.

If the selected parameters in the current screen are not supported by the system, an error message will be displayed on the next page. Go back to the previous screen by pressing the Esc key and select a suitable value for that parameter.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

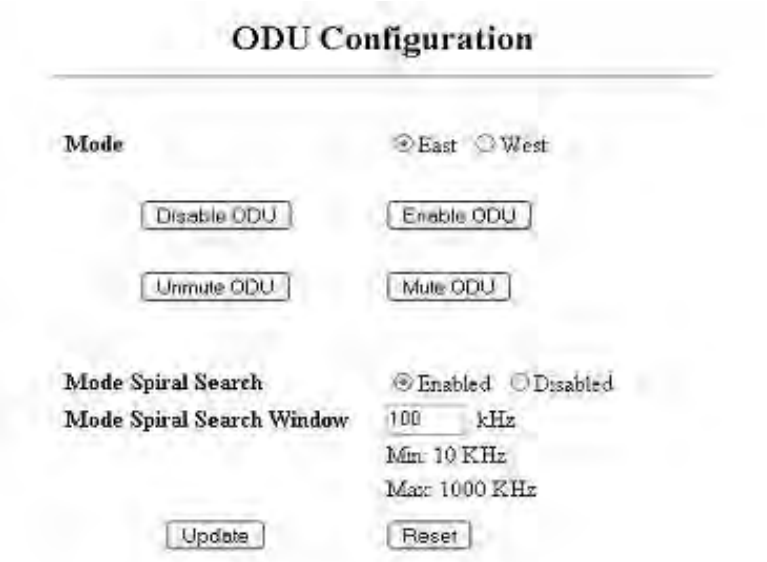
3.3.34.4 SNMP Configuration

1. Select a parameter from the MIB section LinkCfgRadioLinkEastODUCfg
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

Details of the ODU configuration are given below

1. GET the “LinkUtilODUTypeCapability”,
2. Select ODU type gotten above into MIB variables “RadioEastODUCfgType
3. GET the “LinkUtilEastODUChList” MIB variables value
4. SET the channel frequency gotten above into the “RadioEastODUCfgChFreq”.
5. update the ODU configuration by setting the MIB “RadioEastODUCfgChFreqReconfigure”.

3.3.35 ODU Configuration



User Access Level:

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

User Access Level: Level 3

Figure 3.43. ODU Configuration

3.3.35.1 Description

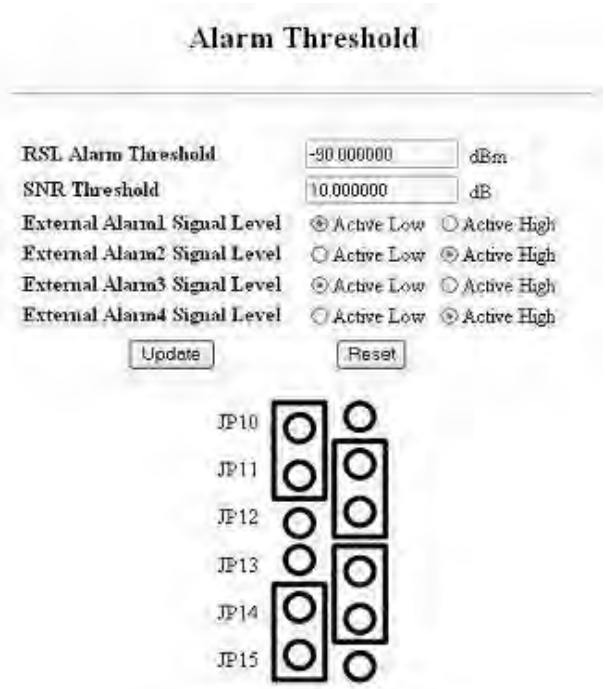
This screen enables the user to configure the ODU (see Figure 3.43).

3.3.35.2 WEB Configuration

1. Click on the radio button to select the ODU (East/West).
2. Press the Disable, Enable, Mute, or Unmute button.
3. In the case of Protected mode, the mute and unmute options will not be available.
4. Click on the radio button to Enable or Disable Spiral Search.
5. The Spiral Search Window value can be entered in the text box and it should be within the range specified.
6. Press the Update button to update the Spiral Search Values.
7. Press the Reset button to reset the Spiral Search Values.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.36 Alarm Threshold



User Access Level:

User Access Level: Level 2

Figure 3.44. Alarm Configuration

3.3.36.1 Description

This screen enables the user to configure the following alarm threshold parameters (see Figure 3.44).

1. **RSL alarm threshold** – Threshold value for **RSL** alarm in ‘dBm’ units.
2. **Signal/Noise threshold** - Threshold value for Signal/Noise alarm in ‘dB’ units.
3. **External alarm signal level** – Active Low or High.

3.3.36.2 WEB Configuration

1. Navigate to Analysis and click on the “Alarm” link in the left panel.
2. Now click on the “Threshold” link.

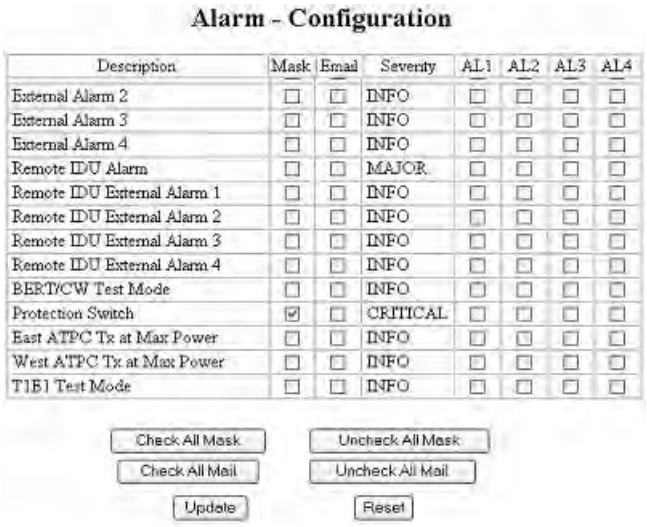
© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3. The alarm threshold parameters will be displayed with current/present values.
4. Change the required parameters and click the “Update” button.
5. The page will be refreshed and displayed with updated values.
6. If parameters are not updated with entered values, the value entered may be invalid for that parameter.
7. Based on the “External Alarm signal level” radio button selection, the External alarm input jumper positions will be displayed.

3.3.36.3 SNMP Configuration

1. Select a parameter from the MIB section AnalysisAlarmThreshold
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

3.3.37 Alarm Configuration



User Access Level: _____

User Access Level: Level 2

Figure 3.45. Alarm Configuration

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.37.1 Description

This screen enables the user to configure the following attributes of the terminal alarms (see Figure 3.45).

1. **Description** – Description of the alarm.
2. **Mask** – masking a particular alarm. If checked ☑ , that particular alarm will be ignored.
3. **E-mail** – If checked ☑ , upon occurrence of this alarm the configured users are notified by E-mail. To configure e-mail parameters, see the e-mail configuration section (Devic)
4. **Severity** – Type of the alarm (Critical, Major and Info).
5. **AL1 – AL4** – Maps alarm output to one of the four external alarm outputs.

3.3.37.2 WEB Configuration

1. Navigate to Analysis and click on the “alarm” link in the left panel.
2. Now click on the “Discrete” link.
3. All alarm attributes will be displayed with current/present values.
4. Change the required parameters and click the “Update” button.
5. The page will be refreshed and displayed with current/present values.
6. All the checkboxes for E-mail notification may be selected by pressing the button “Check All Mails”.
7. All the checkboxes for E-mail notification may be deselected by pressing the button “Clear All Mails”.
8. All the checkboxes for masking the alarms may be selected by pressing the button “Check All Masks”.
9. All the masks may be deselected by pressing the button “Clear All Masks”.
10. If an alarm is active (set), the description of that alarm will be red in color.

3.3.37.3 SNMP Configuration

1. Select a parameter from the MIB section *AnalysisAlarm*, under *Analysis* group
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

Use MIB objects *AlarmMask* and *AlarmEmailMask* for accessing alarm and E-mail masks respectively. Alarm masks will be in the following format

1=U:2=U:1=U:3=U:4=U:5=U:6=U:7=U:8=U:9=U:10=U:11=U:

use “M” to mask the alarm and “U” to unmask the alarm.

3.3.38 Alarm History

User Access Level:

User Access Level: Level 2

Figure 3.46. Alarm History

3.3.38.1 Description

This screen lists alarms that have occurred and their description, status, and time (see Figure 3.46). A maximum of 300 alarms can be displayed. If the alarm history exceeds 300 alarms, the oldest alarms will be removed/overwritten.

The following items are displayed on this page:

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

1. **Description** – Description (name) of the alarm.
2. **Status** – Status of alarm (set/reset).
3. **Time** - The time at which the particular alarm set/reset.
4. **Clear History** – The button used to clear the Alarm History records.

The current alarm state can be obtained from the SNMP manager by reading an MIB object *AlarmStatus* from the *Analysis* section. Status will be returned as string, for example

1=I:2=I:3=I:4=I:5=A:6=I:7=I:8=I:9=I:10=I:11=I:

where “I” indicates that the alarm is inactive and “A” indicates the alarmed state.

3.3.39 Active Alarms

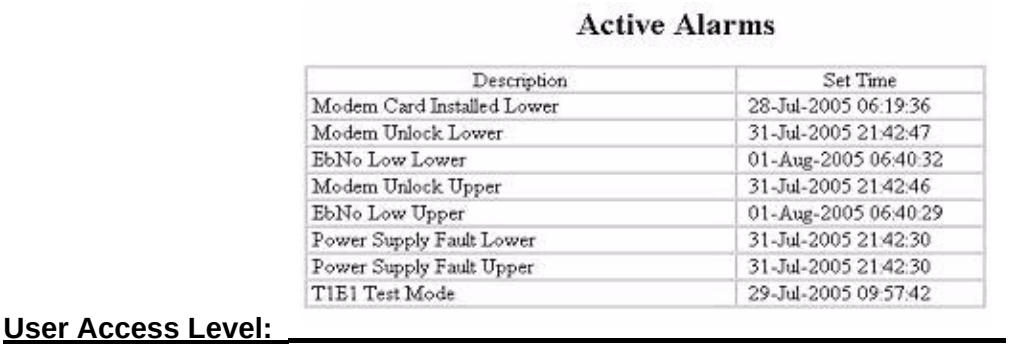


Figure 3.47. Active Alarms

3.3.39.1 Description

This screen shown in Figure 3.47 displays active alarm information including:

1. **Description** – Description (name) of the alarm.
2. **Time** - The time at which this particular alarm set

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.40 Graphs

User Access Level: Level 1

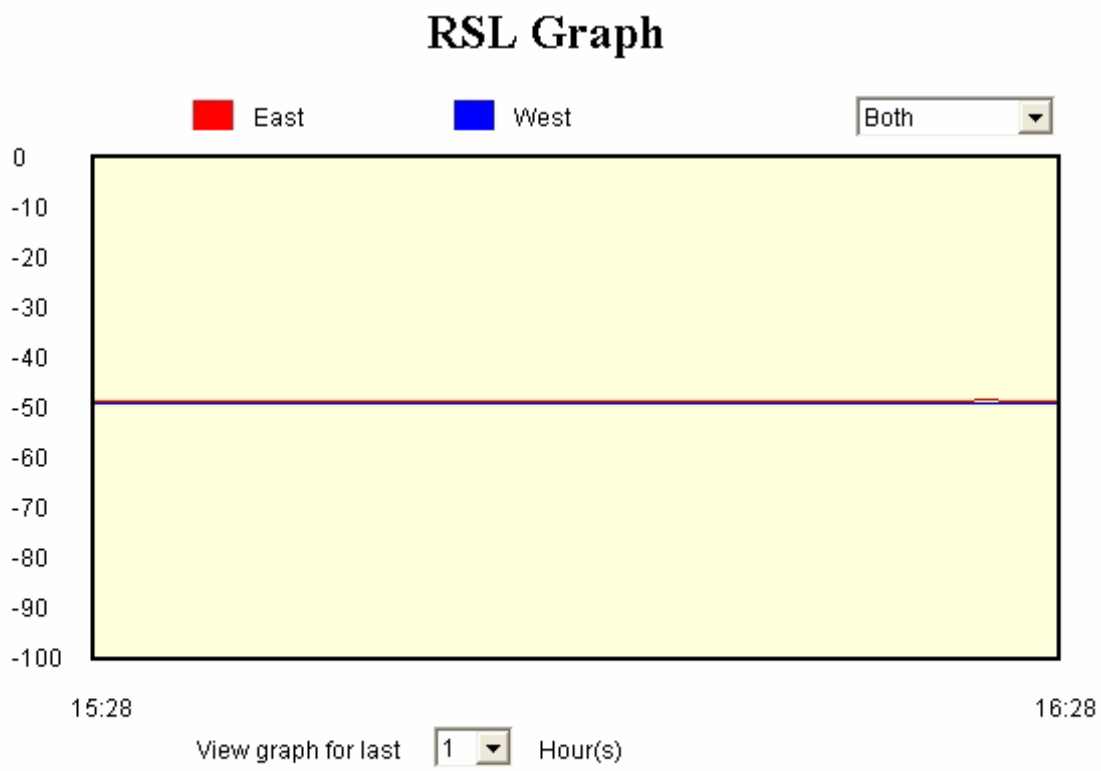
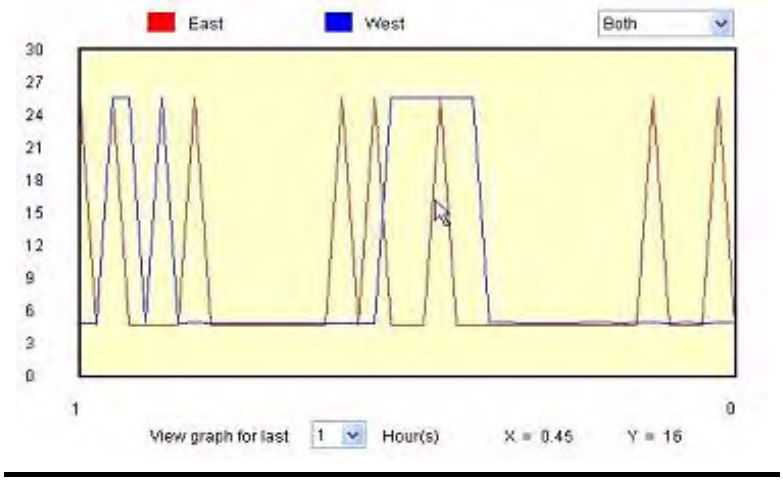


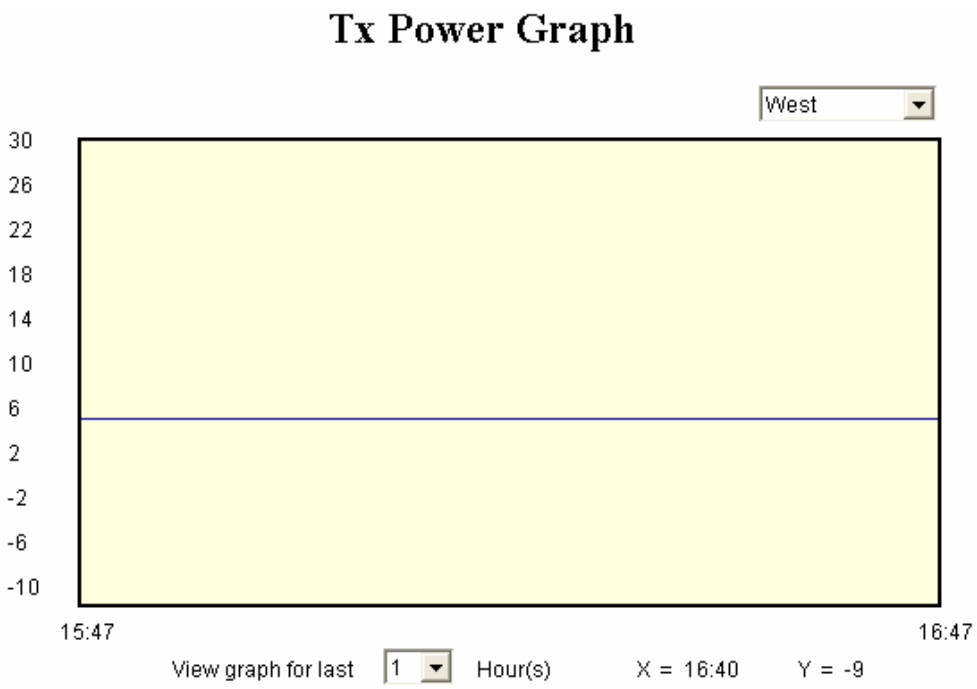
Figure 3-48. RSL Plot.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved



User Access Level: Level 1

Figure 3.49. SNR Plot



X (Horizontal) Axis - Time in Hours
Y (Vertical) Axis - Tx Power in dB

Figure 3.50. Tx Power.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

User Access Level: Level 1

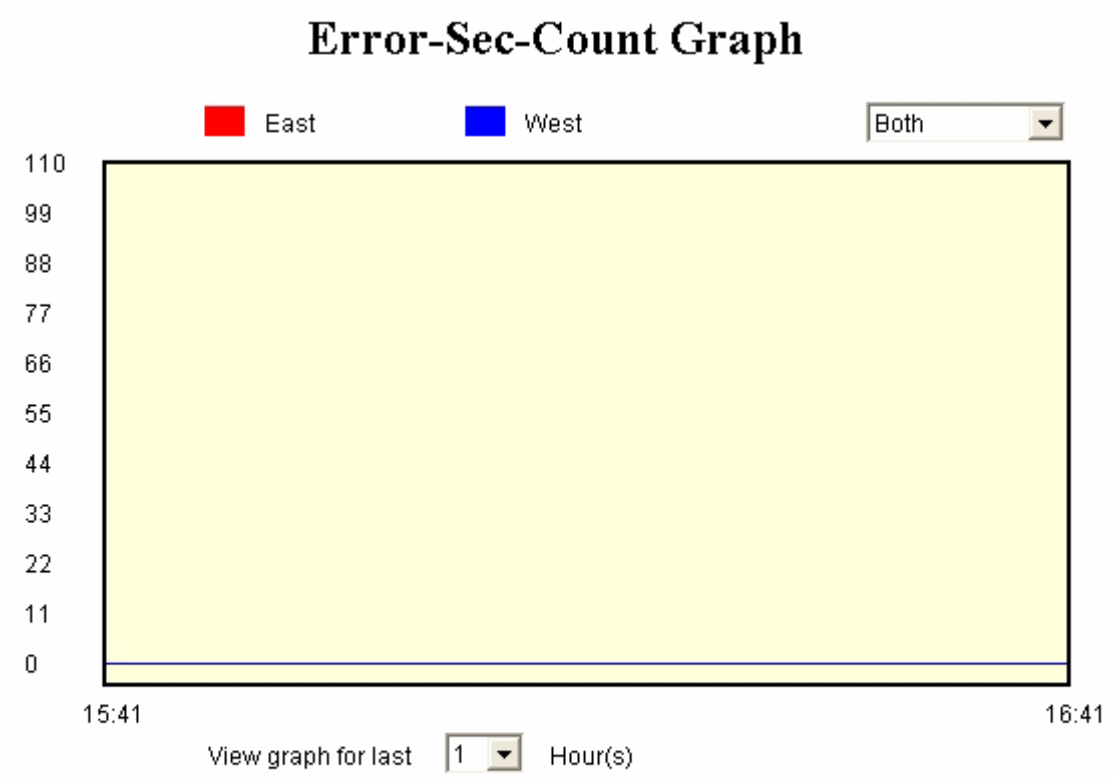


Figure 3.51. Error Seconds Plot.

Note: The algorithm for counting block errors is as follows. The IDU software counts Errored Seconds (ES) and displays the number of errored seconds that occur in a 90 second interval in the graph. An ES is counted if one or more of the modem's internal Reed-Solomon Encoded blocks has an uncorrectable bit error during one second period. The user data BER cannot be calculated directly from the ES because there may be one or more bit errors in an ES.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

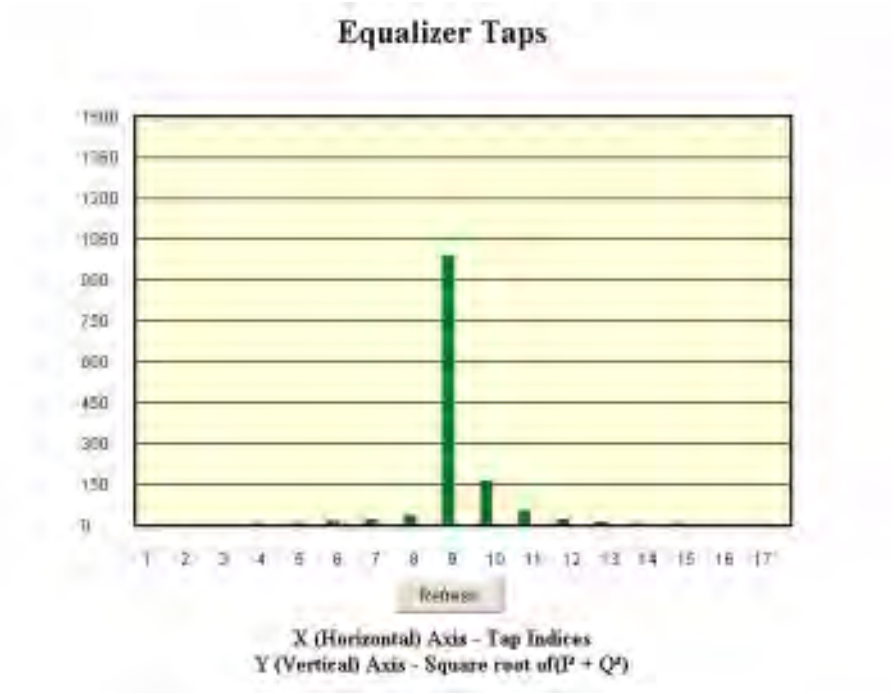


Figure 3.52. Equalizer Taps

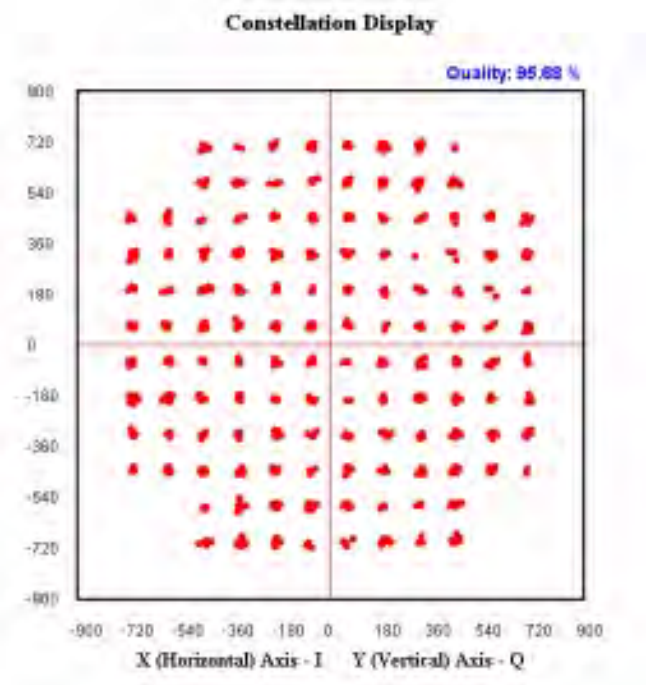


Figure 3.53. Constellation Display (128 QAM)

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.40.1 Description

This screen presents the following parameters graphically:

1. East RSL
2. West RSL
3. East Signal/Noise
4. West Signal/Noise
5. East TX power
6. West TX power
7. East Error second count
8. West Error second count.
9. East Equalizer Taps
10. West Equalizer Taps
11. East Constellation
12. West Constellation

For parameters 1-8, the last 24 hours of data will be plotted with the parameter along the Y-axis (vertical) and time along the X-axis (horizontal) as in Figure 3.49. Equalizer Taps and Constellations are plotted as shown in Figure 3. and Figure 3..

3.3.40.2 WEB Configuration

1. Navigate to Analysis and click on the “Graphs” link in the left panel.
2. Based on the ODU operation mode configuration, the number of graphs displayed will differ. For example, if the ODU operation is East-West, all 8 parameters’ graphs will be accessible. If the ODU operation mode is not East-West, only 4 (either East or West) graphs will be accessible.
3. Select any one link to view the graph of that parameter.
4. The X-axis time range can be selected. (From 1,2,4,12 or 24). If 1 hour is selected, it will plot the graph using last hour of data.
5. When the mouse is moved over the graph area, the corresponding value at the mouse point will be displayed under the graph area. This enables the user to easily read X and Y values.

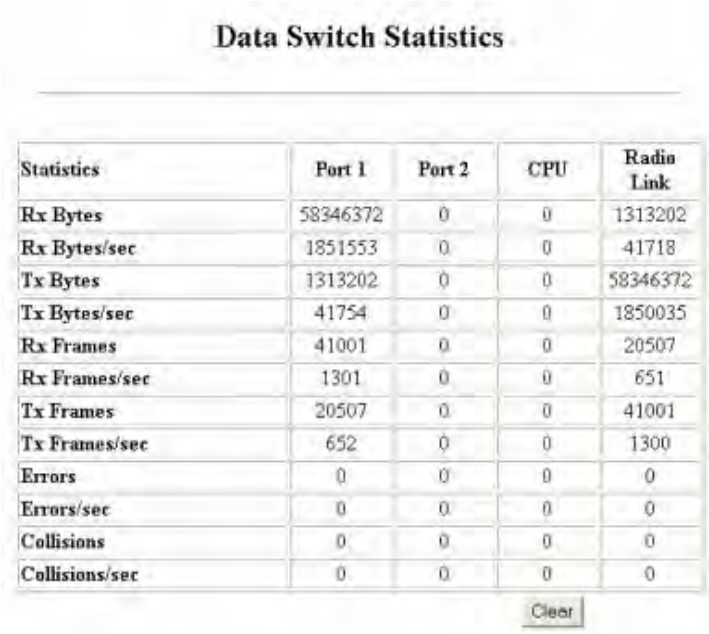
© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.40.3 SNMP Configuration

From SNMP manager graph data can be obtained by reading a MIB object *AnalysisPerfData* from the *Analysis* section._Home

Sometimes an error message may be displayed even for a valid address. The reason is that the requested register is not available for writing and/or reading

3.3.41 Statistics – Data Switch



Data Switch Statistics

Statistics	Port 1	Port 2	CPU	Radio Link
Rx Bytes	58346372	0	0	1313202
Rx Bytes/sec	1851553	0	0	41718
Tx Bytes	1313202	0	0	58346372
Tx Bytes/sec	41754	0	0	1850035
Rx Frames	41001	0	0	20507
Rx Frames/sec	1301	0	0	651
Tx Frames	20507	0	0	41001
Tx Frames/sec	652	0	0	1300
Errors	0	0	0	0
Errors/sec	0	0	0	0
Collisions	0	0	0	0
Collisions/sec	0	0	0	0

Clear

User Access Level:

User Access Level: Level 1

Figure 3.54. Data Switch Statistics

3.3.41.1 Description

This screen provides

1. Rx Bytes
2. Rx Bytes/sec

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3. TX Bytes
4. TX Bytes/sec
5. Rx Frames
6. Rx Frames/sec
7. TX Frames
8. TX Frames/sec
9. Errors
10. Errors/sec
11. Collisions
12. Collisions/sec

for Port 1, Port 2, CPU, Radio Link (East) and Radio Link (West) of the Data Switch, as shown in Figure 3..

3.3.41.2 WEB Configuration

1. Navigate to Analysis -> Statistics and click on the “Data Switch” link in the left panel.
2. Press the “Clear” button to clear the data and start accumulating again.

3.3.41.3 CLI Configuration

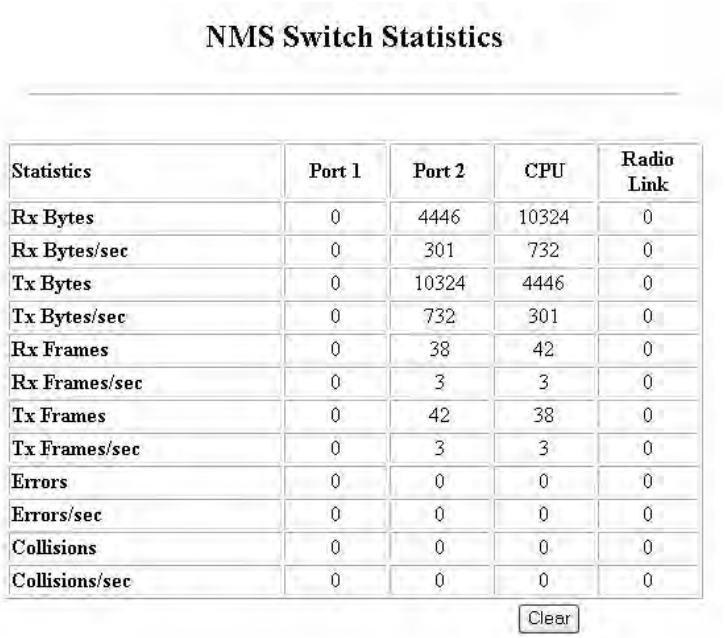
Navigate to Analysis -> Data Switch Statistics

3.3.41.4 SNMP Configuration

1. Select a parameter from the MIB section *AnalysisUPLSwitch*
2. Use the SNMP GET command to get the value of the required parameter
3. The SNMP agent will return the actual value on successful get operation. Upon failure, the SNMP agent will return an error if agent is not able to get the value or the user does not have access rights to the selected parameter.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.42 Statistics – NMS Switch



NMS Switch Statistics

Statistics	Port 1	Port 2	CPU	Radio Link
Rx Bytes	0	4446	10324	0
Rx Bytes/sec	0	301	732	0
Tx Bytes	0	10324	4446	0
Tx Bytes/sec	0	732	301	0
Rx Frames	0	38	42	0
Rx Frames/sec	0	3	3	0
Tx Frames	0	42	38	0
Tx Frames/sec	0	3	3	0
Errors	0	0	0	0
Errors/sec	0	0	0	0
Collisions	0	0	0	0
Collisions/sec	0	0	0	0

Clear

User Access Level:

User Access Level: Level 1

Figure 3.55. NMS Switch Statistics

3.3.42.1 Description

This screen provides

1. Rx Bytes
2. Rx Bytes/sec
3. TX Bytes
4. TX Bytes/sec
5. Rx Frames
6. Rx Frames/sec
7. TX Frames
8. TX Frames/sec
9. Errors
10. Errors/sec
11. Collisions

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

12. Collisions/sec

for Port 1, Port 2, CPU, Radio Link (East) and Radio Link (West) of the NMS Switch, as shown in Figure 3..

3.3.42.2 WEB Configuration

1. Navigate to Analysis -> Statistics and click on the “NMS Switch” link in the left panel.
2. Press the “Clear” button to clear the data and start accumulating again.

3.3.42.3 CLI Configuration

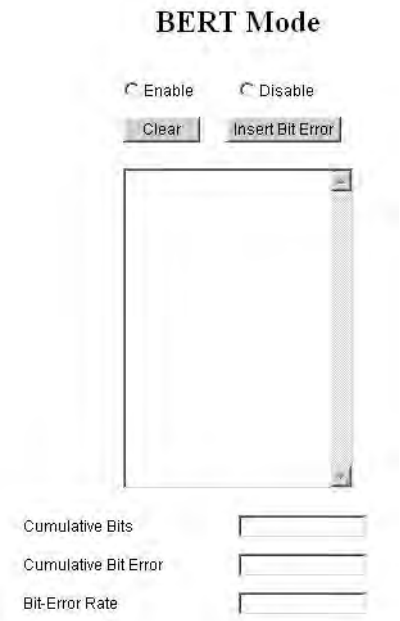
Navigate to Analysis -> SNMP Switch Statistics

3.3.42.4 SNMP Configuration

1. Select a parameter from the MIB section *AnalysisNMSSwitch*
2. Use the SNMP GET command to get the value of the required parameter
3. The SNMP agent will return the actual value on successful get operation. Upon failure, the SNMP agent will return an error if agent is not able to get the value or the user does not have access rights to the selected parameter.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.43 BERT Mode



User Access Level:

User Access Level: Level 2

Figure 3.56. BERT Mode

3.3.43.1 Description

This screen is used to communicate with the MODEM directly by sending a command and receiving the response (see Figure 3.).

The following items are displayed

1. **Command selection** – For Selecting East/west and Enable/Disable.
2. **“Clear” button** – send the “clear” command to the MODEM.
3. **Text Area** – To display the response messages from MODEM.

To use the CFQ IDU BERT capabilities, the BERT mode has to be enabled independently at both ends of the link because there is no separate NMS stream when operating in BERT mode. This will require the use of two PCs, one connected directly to the NMS port of each IDU.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.43.2 WEB Configuration

To begin testing:

1. Navigate to Analysis and click on the “BERT mode” in the left panel.
2. Enable one of the IDU’s BERT mode
   a. Click on one command. (East Enable or West Enable).
   b. After few seconds (depending on your network speed) the response from MODEM for the given command will be displayed in the text area.
   c. Enabling this mode will generate random data over the link causing the other IDU to trigger the buzzer, generating noise.
3. Enable the other IDU's BERT mode. This should silence the buzzer noise.
4. Send the “Clear” command to both IDUs to reset the cumulative bits, cumulative bit errors, and bit error rate counters.
   a. Click on the “Clear” button.
   b. After few seconds (depending on your network speed) the response from MODEM for the given command will be displayed in the text area.
5. Every time the response message will be appended at the end, so using the scroll bar you can see all messages.

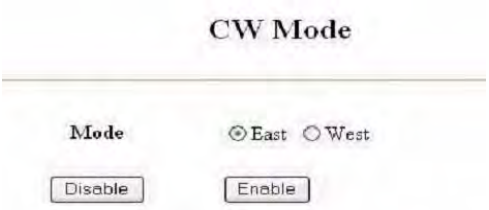
To stop testing:

1. Disable one of the IDU's BERT mode.
   a. Click on one command. (East Disable or West Disable),
   b. This will cause this IDU to generate buzzer noise.
2. Disable the other IDU's BERT mode, this should silence the buzzer noise.

Number of Bits, Bit Errors, and BER will be accumulated until the BERTs are disabled, or the IDUs are power cycled, which will clear the BERT mode.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.44 CW Mode



User Access Level:

User Access Level: Level 2

Figure 3.57. CW Mode

3.3.44.1 Description

This screen allows the user to enable or disable CW mode (see Figure 3.).

3.3.44.2 WEB Configuration

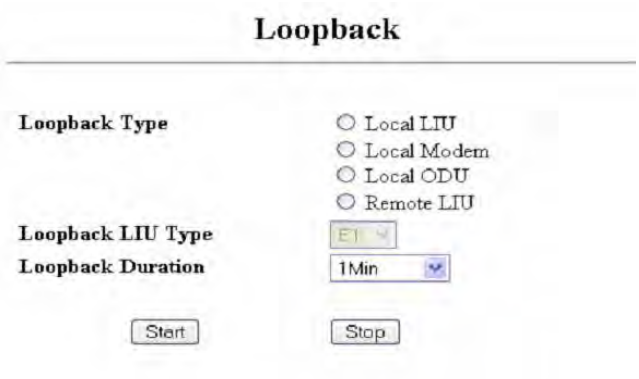
Select required mode (East/West) and press the “Enable” or “Disable” button. A status message will be displayed to indicate success/failure. When CW mode is enabled, the transmitter status in the “status panel” (Right side panel) will display “CW Mode”.

3.3.44.3 SNMP Configuration

1. Select a parameter from the MIB section *AnalysisModemConfig*
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.45 Loopback



User Access Level:

User Access Level: Level 2

Figure 3.58. Loopback

3.3.45.1 Description

This screen enables the user to start or stop Loop Back (see Figure 3.).

3.3.45.2 WEB Configuration

1. Navigate to Analysis→Loopback.
2. Select the type of loopback (Local LIU, Local Modem, Local ODU or Remote LIU).
3. If Local or Remote LIU is selected then select the LIU type from the drop down option.
4. Select the duration of the loopback.
5. Press the start Button to start loopback.
6. If loopback is running, press the stop button to stop it.

3.3.45.3 CLI Configuration

1. Navigate to Analysis→ LoopBack.
2. Select the type of loopback (Local LIU, Local Modem, Local ODU or Remote LIU) by pressing appropriate hotkey and the space bar.
3. If Local or Remote LIU is selected then select the LIU type.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

4. Select the duration of the loopback by pressing appropriate hotkey and the space bar.
5. To start loopback, press the hotkey for Start.
6. To revert to the previous value, press the “Esc” key while editing the value
7. If loopback is running, press the hotkey for stop to stop it.

3.3.45.4 SNMP Configuration

1. Select a parameter from the MIB section *AnalysisLoopback*
2. Use the SNMP GET command to get the value of the required parameter
3. Use the SNMP SET command to set the value of the required parameter
4. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error if the value set is out of range, or the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

3.3.46 Modem Temperature

3.3.46.1 SNMP Configuration

1. Select a parameter (*ModemEastTemperature* or *Modem* West Temperature) from the MIB section *AnalysisModemConfig*
2. Use the SNMP GET command to get the value of the required parameter
3. The SNMP agent will return the actual value upon successful set or get operation. Upon failure, the SNMP agent will return an error the agent is not able to get or set the value, or the user does not have access rights to the selected parameter

3.3.47 Logout:

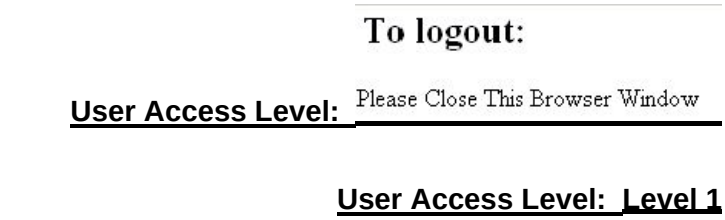


Figure 3.59. Logout

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

3.3.47.1 Description

The page shown in Figure 3. enables the user to logout from the Web Interface. In the case of Internet Explorer, the logout link will close the browser. For other browsers, the user may have to close and reopen the browser.

3.4 Uploading Files to IDU

The file upload may be necessary to

- Upgrade IDU firmware files,
- Change ODU channel plans (file *channel.img*), or
- Change IDU configuration modes (file *modes.img*).

The file upload is performed by connecting to CFQ IDU FTP server; the files can be uploaded in the following ways:

- Using iPorter software, or
- Using Internet browser

3.4.1 File Upload using *iPorter* Program

To upload new firmware file(s) (*.pkg* file) using iPorter program, please refer to the *CFQ Digital Radio User Reference and Installation Manual*.

3.4.2 File Upload using Internet Browser

To upload channel file (*channel.img*) or IDU operation mode file (*modes.img*), proceed as follows:

- Connect a PC to CFQ IDU Ethernet management port
- Open Internet browser program and in address bar type *ftp:**xxx.xxx.xxx.xxx* , where xxx.xxx.xxx.xxx – IDU management port IP address.
- Enter username and password for administrator or integrator user level, for default username and password for each user level please refer to chapter 2.2.
- *Copy-Paste* or *Drag-and-Drop* the firmware files as needed.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

4 Troubleshooting

4.1 Cannot access IDU using IP (Web / Telnet / SSH)

- Verify the IP Address or Hostname of IDU
- Determine if the terminal is up by pinging the IDU
- Check your PC's Network Configuration
- Check Cables

4.2 The web page resolution is improper

- The pages are best viewed at resolutions of 1024x768 or greater
- The pages are best viewed using Microsoft Internet Explorer Version 5.5 and above.

4.3 Unable to establish a secure connection

- Ensure that the HTTP Access in the Security Configuration of the system is set to HTTP (SSL)
- Check if "Use SSL 2.0" and "Use SSL 3.0" options are selected in the Security Options of the browser

4.4 Unable to access different network services

- Telnet

    1. Verify possibilities mentioned in Log.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

2. Telnet may be disabled.

- SSH

1. Verify possibilities mentioned in Log
2. SSH may be disabled

- Serial

1. Verify the serial cable and proper connection.
2. Serial port may be disabled.

- WEB

1. Verify possibilities mentioned in Log
2. HTTP / Secure-HTTP access may be disabled.

By default, the User can logon through

- SSH
- Web https support
- SNMP Manager.

These interfaces can be configured in

1. the “Security Configuration Screen” as
   a. Command Line Interface – Telnet / SSH / Disabled
   b. HTTP Access – HTTP With SSL / HTTP Without SSL / Disabled
2. the “Serial Configuration Screen” as
   a. Device Selection – Modem with IP / Modem Without IP / RS232 / Disabled.

Care should be taken not to disable all three interfaces.

If all three interfaces are disabled, load a new configuration from the Bootloader prompt at the installed site.

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

5 Appendix

5.1 Abbreviations & Acronyms

AES	Advanced Encryption Standard
AIS	Alarm Indication Signal
APC	Automatic Power Control
BER	Bit Error Rate
CLI	Command Line Interface
Codec	Coder-Decoder
DB	Decibel
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
Eb/No	Signal-to-Noise Ratio
FPGA	Field Programmable Gate Array
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HT	high-band transmit
HTML	Hyper Text Mark-up Language
HTTP	Hyper Text Transfer Protocol
IDU	Indoor Unit

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

IE	Internet Explorer
IF	Intermediate frequency
IP	Internet Protocol
JVM	Java Virtual Machine
LED	Light-emitting diode
LIU	Line Interface Unit
LOS	Line of Sight
LT	Low-band transmit
MAC	Media Access Control
MIB	Management Information Base
Modem	Modulator-demodulator
NMS	Network Management System
NTP	Network Time Protocol
OC-3	Optical Carrier level 3
ODU	Outdoor Unit
PPPD	Point-To-Point Protocol Daemon
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RSL	Received Signal Level (in dBm)
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

SNR	Signal-to-Noise Ratio
SNTP	Simple Network Time Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
STM-1	Synchronous Transport Module 1
STP	Spanning Tree Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TX	Transmitter
UI	User Interface

5.2 References and Links

5.2.1 Install Mozilla Firefox

- Visit
  http://www.mozilla.com/firefox/
- Click on “Download FIrefox” to download the installation package
- Run the downloaded executable and follow installation instructions

5.2.2 Install Internet Explorer

- Visit
  http://www.microsoft.com/windows/ie/
- Click on “Downloads” and select an appropriate version to download
- Run the downloaded executable and follow installation instructions

© Copyright 2009 SAF Tehnika A/S All Rights Reserved

5.2.3 Install Java

- Visit

  http://www.java.com/

- Click on “Download Now” to download the installation package
- Run the downloaded executable and follow installation instructions

5.2.4 Install PuTTY

- Visit

  http://www.puttyssh.org/

- Click on “Download ”
- Click on the appropriate version for your platform to download the installation package
- Run the downloaded executable and follow installation instructions

© Copyright 2009 SAF Tehnika A/S All Rights Reserved